open for business

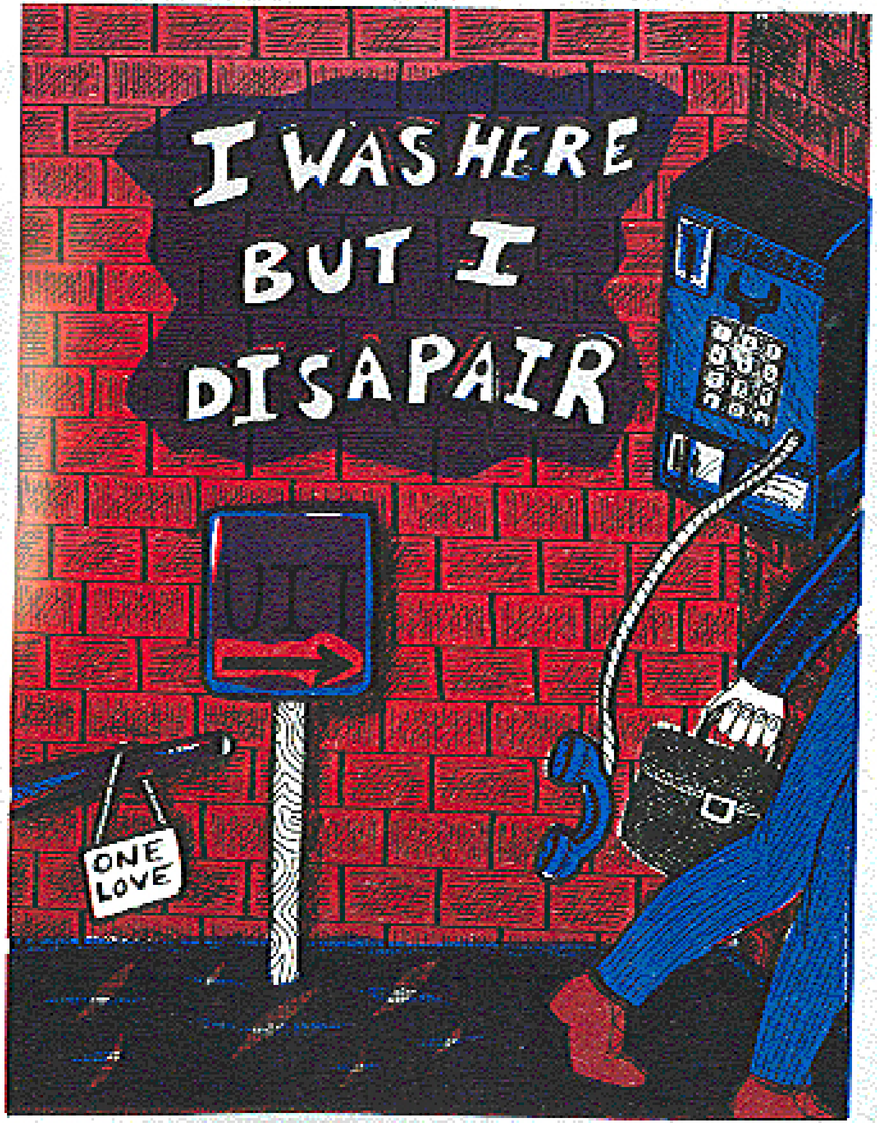
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

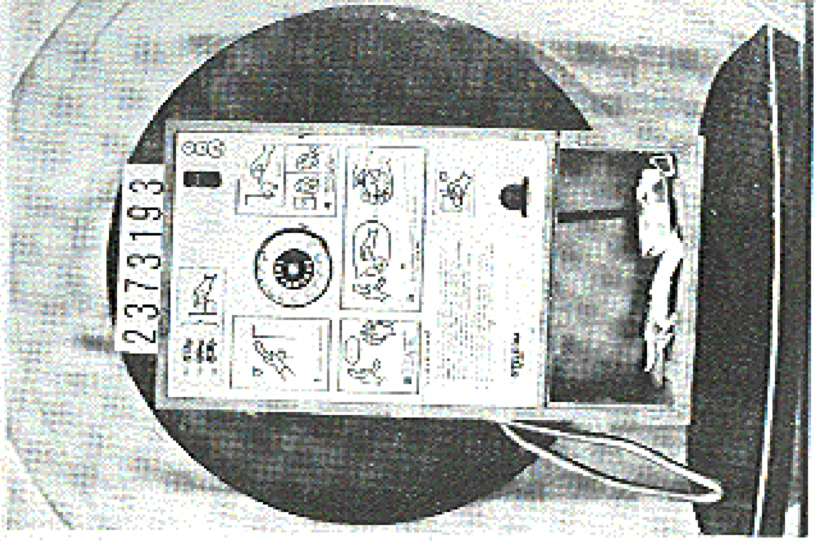
2600

MERELY EXTENDED FREEDOM IS PRIVILEGE
IS MERELY FREEDOM EXTENDED PRIVILEGE
FREEDOM MERELY EXTENDED IS PRIVILEGE
EXTENDED FREEDOM IS PRIVILEGE MERELY
IS PRIVILEGE MERELY EXTENDED FREEDOM
PRIVILEGE IS FREEDOM EXTENDED MERELY
FREEDOM IS MERELY PRIVILEGE EXTENDED
MERELY PRIVILEGE IS EXTENDED FREEDOM
MERELY FREEDOM IS EXTENDED PRIVILEGE
EXTENDED IS FREEDOM MERELY PRIVILEGE

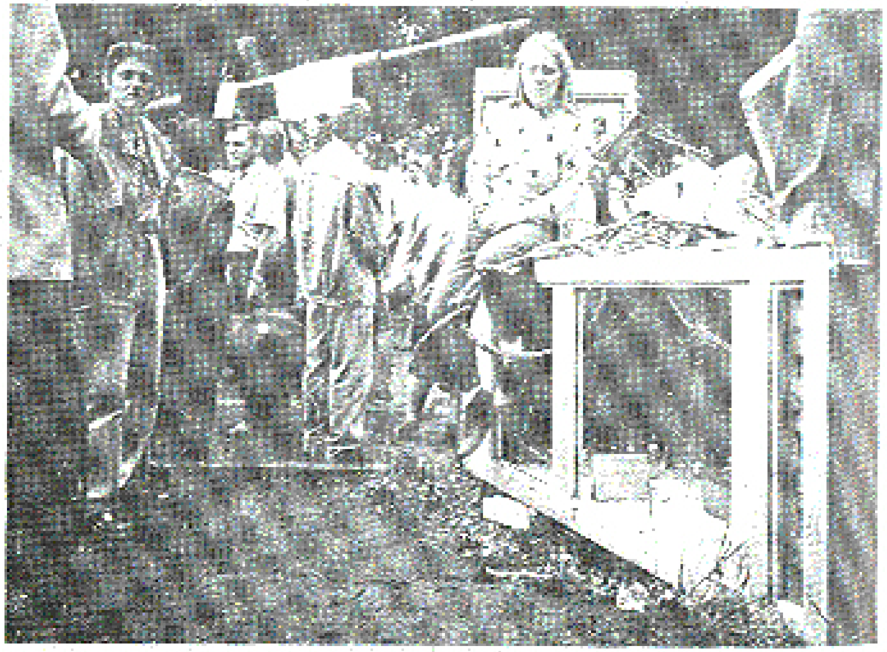
The Hacker Quarterly

VOLUME EIGHT, NUMBER TWO
SUMMER, 1991





This is a Czechoslovakian payphone. It will take a few minutes for your eyes to adjust. This is a normal reaction.



Brave 2600 photographers risked certain death recently in the Soviet Union to bring you exclusive pictures of a Soviet payphone being used as a barricade against tanks during the recent coup attempt.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. STILL WAITING FOR AFRICAN PAYPHONES.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada -- $21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990
at $25 per year, $30 per year overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
NETWORK ADDRESS: 2600@well.sf.ca.us

2600 **Office Line: 516-751-2600,** *2600* **FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, Bob Hardy, The Infidel, Kevin Mitnick, Knight Lightning, The Devil's Advocate, The Plague, David Ruderman, Bernie S., Silent Switchman, Mr. Upsetter, Dr. Williams, and the nameless masses.

Remote Observations: Geo. C. Tilyou

Shout Outs: Ivan, Bob, Franklin, KGB.

[illegible]

Where Have All The Hackers Gone?

This is one of the more common questions circulating today. Only a couple of years ago, things seemed very different. Hacker bulletin boards were everywhere. Knowledge was spread freely on a multitude of topics, from telephone switches to all of the latest operating systems. Looking back, it all seemed so magical.

So what has changed? Two things primarily. One, naturally, is the technology itself. Antiquated telephone equipment is rapidly becoming a memory, to be replaced by sleek, modern paraphernalia that too often seems to miss the point entirely. Computers are becoming increasingly integrated into our everyday lives. The other change, however, is more troublesome. The people who make up our unique community are becoming affected by the draconian measures of a misguided few who are determined to rid technology of hackers, apparently at almost any cost.

We've seen many innocent people victimized in countless hacker hunts. Bulletin board operators who allowed hackers to communicate have repeatedly found themselves the targets of raids by government agencies, even though they themselves were not hackers. It happened to our own system operator in July of 1985. Other examples include parents returning home to find their front doors smashed in by the Secret Service, their child having been suspected of being a hacker. In some cases, no charges were ever filed. Yet much that had been confiscated was never returned. More recently, goons from the New York State Police forced their way into a Manhattan apartment, apparently believing that the best way to calm down an hysterical parent was to reveal their shotgun. Not surprisingly, this didn't work.

The absurdities and indignities that decent people have been subjected to in the search to weed out the hackers could fill every page of this publication. In the beginning, it was easy to laugh when confused government agents confiscated TV sets and rotary telephones. But the mood has slowly been changing over the years. People are really getting hurt now. Students are being taken out of school and sent to prison for such offenses as copying files, accessing systems that had no password protection, or just being mischievous. It's reached the point where their "crimes" are viewed by some as more worthy of punishment than crimes of violence, primarily because of the potential for damage if they decided to be malicious. The fact that the overwhelming majority of hackers are not malicious is simply brushed aside as is the weak security that allows easy access to so many.

We can't say we're surprised. As soon as it became clear that our courts were primarily interested in protecting corporate rights, it was only a matter of time before individuals began paying a heavy price.

Let's examine the facts. An individual cannot take TRW to court because they collect personal data on the individual without his/her permission. But TRW can claim its privacy was violated if a hacker figures out how to access the system. Ironically, most people didn't even know what TRW was doing until hackers revealed the system back in 1984.

When IBM's Prodigy recently was found to have faulty software that gave the appearance that they were able to read personal files on users' computers, they explained themselves and everybody listened. But a hacker found with a corporate document on his system is given no such luxury. It's assumed that he was up to no good and he is treated like a criminal.

Bell South is able to put people in jail for absurd, trumped up charges. (The Atlanta hackers were imprisoned for merely accessing a system that had no password!) Yet Bell South is caught red-handed lying about the value of a document in court. (The 911 document that they claimed was worth $80,000 was actually worth less than $15.) The ridiculous pricing scheme they use to justify their actions (revealed on page 6) is believed without question. But if an individual whose life has been shattered by this corruption wishes to be compensated, he soon learns how impossible justice is becoming.

Again, there are countless examples of corporate "privacy" being protected at the expense of individual liberty. It's a very frightening scenario and we have to wonder how long it will take for mainstream society to see the threat. Now that we live in the world's only superpower, what or who will become the new enemy?

All of this is a bit much for the average hacker to take. It's not surprising to see people keeping a low profile. But inertia cannot be forgiven. Things are changing all around us and by allowing what is clearly wrong to take place, we are as guilty as if we had done it ourselves.

Freedom of speech must be preserved at any cost. You can still exercise that right in a very meaningful way by running a computer bulletin board where people can communicate freely. You may get your door kicked in if government agents or corporate security people don't like or understand what is being said. You may get a file started on you. But it's a risk you must be willing to take. After all, what is the alternative? If we continue down this road, restrictions on speech and assembly will extend beyond the world of computers and into our everyday lives. If registration of bulletin boards with the government becomes the norm, newspapers and magazines will be next. If you doubt this, consider the fact that there are more electronic newspapers and magazines emerging every year.

Admittedly, a lot of us are really only interested in learning. It makes sense not to get involved in all of this crap. But the fact is that we have become pawns in a much larger game. To submit to unacceptable terms and remain underground like criminals is the worst thing that can happen to the hacking community.

We have to accentuate the positive elements that once were so common. As well as an increase in boards, we want to see more people writing from the hacker perspective. The hundreds of legendary files about various operating systems need to be updated and rewritten. There are an incredible number of topics waiting to be tackled. There are also many people who want to learn about technology from an individual perspective but don't know how to begin. The key is to share information. The rest will follow.

We must also get rid of our negative tendencies. The most prevalent of these is the habit of suppressing information. It's a double standard to be on a quest for knowledge and then keep it to yourself when you obtain it. It's also self-defeating. And it's playing the same game that the people who stand against us are playing. There are an incredible number of people who want to learn, not just share results. A populace that knows how to manipulate technology to its advantage will result in a much healthier society. The opposite is too terrifying to even contemplate. We are in the unique position of greatly influencing which becomes reality.

"Elite" hackers and hacker "gangs" do more harm than good in the big picture. Egos and machismo tend to cloud the reason we got involved in the first place. They also serve as the means to lock out others. And, of course, anybody who crashes systems, wipes data, or does anything malicious for no apparent reason is doing more against hackers than any government agency ever could. Fortunately, these kind of people are extremely scarce in the hacker world, a fact that speaks volumes.

Another form of elitism can be found in older hackers who want to distance themselves from what the younger hackers are doing. They believe the way to do this is to create a new label for the "undesirables" and call them "crackers". It's an ill-conceived attempt at manipulation that simply serves to split the community. This description of hackers comes from the book *Cyberpunk* (reviewed on page 42): "The earliest self-described computer hackers, those at MIT who abhorred computer security, or anything else that would inhibit the sharing of information and free access to computers, had it in for Multics from the start. MIT hackers often tried to bring the system to its knees, and occasionally they succeeded." Those were the "old-style" hackers, not the "young punks" of today. The fact is, we all speak a common language. While there are many different forms of hacking, further categorization is *not* the answer.

Where have all the hackers gone? They haven't really gone anywhere, although some would like you to believe they have. There are more hackers today than ever before. But they are becoming invisible out of fear. We hope to see more people do whatever they can to get ideas and information flowing again. The strength of our efforts will determine whether we move into new and uncharted territory or simply repeat history yet again.

The following letter is what started the entire 911 document fiasco in 1990. It explains how the worth of the document was calculated at $79,449. Note that full salaries and an entire computer system were included as part of the expense incurred in creating the document. Such wanton fraud and exaggeration is criminal in itself. The fact that the United States government accepted these preposterous figures without question is clear proof of whose interests are being protected - at whatever cost.

This document was originally printed in EFFector Online 1.10.

BellSouth
1155 Peachtree Street, N E
Atlanta, Georgia 30367-6000

January 10, 1990
Bill Cook - Assistant United States Attorney
United States Attorney's Office
Chicago, Illinois
Dear Mr. Cook:

Per your request, I have attached a breakdown of the costs associated with the production of the BellSouth Standard Practice (BSP) numbered 660-225-104SV. That practice is BellSouth Proprietary Information and is not for disclosure outside BellSouth.

Should you require more information or clarification, please contact my office at XXX-XXX-XXXX. FAX: XXX-XXX-XXXX

Sincerely,
Kimberly Megahee
Staff Manager - Security, Southern Bell

[Handwritten total]
17,099
37,850
24,500
79,449

[Attachment to letter itemizing expenses]

DOCUMENTATION MANAGEMENT

1. Technical Writer To Write/Research Document
-200 hrs x 35 = $7,000 (Contract Writer)
-200 hrs x 31 = $6,200 (Paygrade 3 Project Mgr)

2. Formatting/Typing Time
-Typing WS14 = 1 week = $721.00
-Formatting WS 14 = 1 week = $721.00
-Formatting Graphics WS16 = 1 week = $742.00

3. Editing Time
-PG2 = 2 days x $94.48 = $387

4. Order Labels (Cost) = $5.00

5. Prepare Purchase Order
-Rice Number Practice WS14 x 1 hr = $18.00
-Type PO WS10 x 1 hr = $17.00
-Get Signature (PG2 x 1 hr = $25.00)
(PG3 x hr = $31.00)
(PG8 x 1 hr = $38.00)

6. Printing and Mailing Costs
Printing= $313.00
Mailing WS10 x 50 hrs = $858.00
(Minimum of 50 locations/ 1 hr per location/ 115 copies

7. Place Document on Index
-PG2 x 1 hr = $25.00
-WS14 x 1 hr = $18.00

Total Costs for involvement = $17,099.

HARDWARE EXPENSES	
VT220	$850
Vaxstation II	$31,000
Printer	$6,000
Maintenance	10% of costs

SOFTWARE EXPENSES	
Interleaf Software	$22,000
VMS Software	$2,500
Software Maintenance	10% of costs

magnetic stripes

Translated from Hack-Tic, #8, 49-50, available at PO box 22953, 1100 DC Amsterdam, The Netherlands.

by Dr. Abuse

Cash is out. Plastic is in. In the nineties, the question is: who has the best hand of cards? We will help you to have the fifth ace by giving you the opportunity to play the big magnetic card game.

Everybody has looked at those credit cards and wondered what exactly was on them. Whoever dared to even ask about magnetic reader/writers was shocked after hearing the price and they went back to their daily living. And this while you would be very anxious to know what the bits and bytes mean.

We now give you the opportunity to build your own credit card reader/writer. For the cost of playing around with electronics plus a few dollars, you can build your own magnetic card copier. This device reads from one magnetic card and puts the data out onto the other card. For the advanced electronic hobbyist, there is the magnetic card reader and writer. Everybody who knows what TTL is and can squeeze something out of his computer and/or hold a soldering iron will be able to make this credit card reader/writer together with the schematics.

Far more interesting than all of the electronic mumbo-jumbo is to first see what's really on the magnetic stripe. For that we give you the first bit of information in this article.

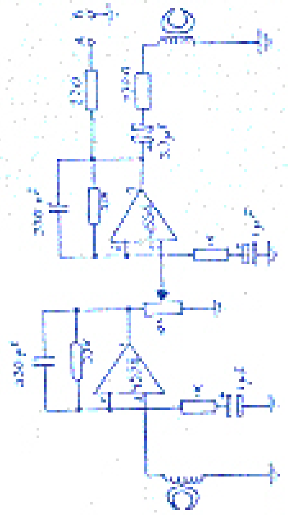
The information on most credit cards is stored in binary form. These ones and zeros are stored by changing the magnetic field of the magnetic head by 180 degrees. To see what's really on the card, you put some iron filings on the magnetic strip and tap the card gently onto the edge of the table (keep paper underneath it because it probably would have cost you lots of effort to make the iron filings) and behold! Here's your magnetic information, plainly visible to the eye. Some cards have such big bits that you theoretically should be able to change the information on it with a magnetized razor blade (Paris Metro cards are a good example). On other cards, the bits are so close to each other that you will only see a magnetized solid bar.

To store away the information on magnetic cards, some international standards were developed by ISO - the International Standards Organization. To name one: the magnetic stripe is divided up into three tracks. A lot of manufacturers use other coding methods to write the cards with and only the iron filing method will give you insight as to what's on the card in these instances.

The first project as mentioned before is to copy the information from one magnetic card to another. This means that it doesn't matter whether the information is encoded or not since you are just copying it. The only thing you need to know is the exact location and height of the track with the information that you want to copy. As long as the write head of your copier is bigger than the magnetic strip, you are safe. See the schematic on this page.

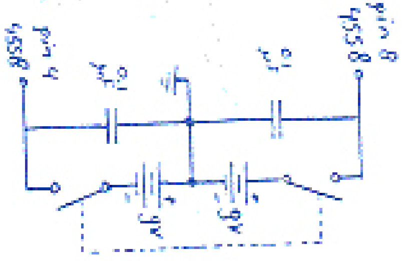
The Credit Card Copier

At the left of the schematic you will see the read head. For this (as well as the write head) you cannot use any cassette player head which happens to be lying around. You will need to use a data head or a card reader head (you can obtain them from Michigan Magnetics among others). If the head is bigger than the track you are reading from, you will pick up extra noise but if the head is too small, the signal might become too weak. Experimenting with the gain is essential. The write head should be as big as possible unless you want to write more than two narrow tracks next to each other. Between points A and B you can put a pair of headphones (which you have put in series). If you pass the read head along the stripe, you will hear a sound that might be familiar to you hobbyists who used to once work with data cassettes. Now you will need to find a way to make the read and write head go simultaneously along both cards. The trick for this is to take a piece of wood and mount both heads on both ends of it. Attach the cards (with scotch tape) to a solid surface and gently slide the heads along both cards (making sure that the heads go in parallel with the magnetic stripe).



There are, however, cards on which the information is not put on the stripe at a ninety degree angle. If you see something like that (using the iron filing method) you will have to adjust the position on which the heads are mounted. A little trick to adjust the heads is to replace the 220 ohms resistor in front of the headphones by a 100 nF capacitor and then listening until you find the angle that gives you the highest pitch sound.

You can only write to a card which you have erased previously by, for instance, a demagnetizer. To doublecheck if your copy is good, you can listen to it by passing the read head over it and checking to see if the sound of the original and the copy are the same. We found out that the human ear is a very accurate meter to indicate the accuracy of the copy. One last word about the dual opamp - pins 4 and 8 of that chip are used to supply positive and negative voltage. (See drawing below.)

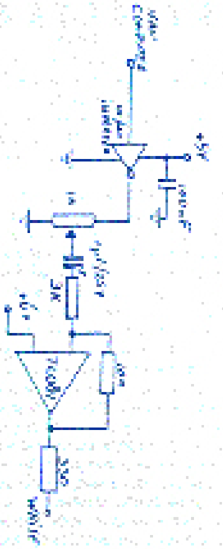


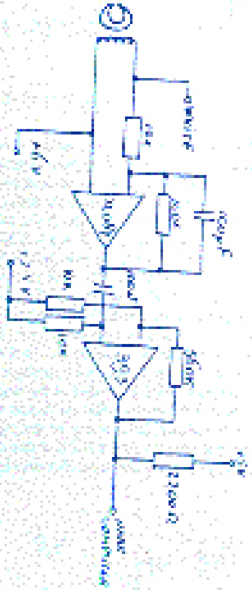
The Reader/Writer

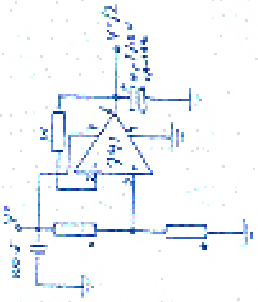
This schematic reads and writes to the same head. If you want to write something with this schematic, you will have to come up with a device which has a very accurate constant speed, like a modified printer. The most suitable device, though, would be a real reader/writer mechanism.

Most opamps want to have a positive as well as a negative voltage. But by means of an active voltage divider (see drawing) we can supply the whole card reader from one 12 volt power supply. The active voltage divider is used twice in the reader/writer. First of all to divide the 12 volt down to six volts (in order to do this you put a 6.8 kohm resistor where the asterisks are in the schematic). The second voltage divider you make by putting a 3.3 kohm resistor at that spot. This is done to divide the 5 volts out of your computer into 2 1/2 volts. The best thing to do is to place a relay on the write line going to the head. This is so as not to introduce noise while reading from the card.

Now all you need is an interface that can control the motor of your read/write unit and which can exchange the bits with the circuitry described above. What you can do then is make binary copies of your card. The credit card reader/writer can only be used on cards which store their information in binary form, so go and check first with the iron filings.







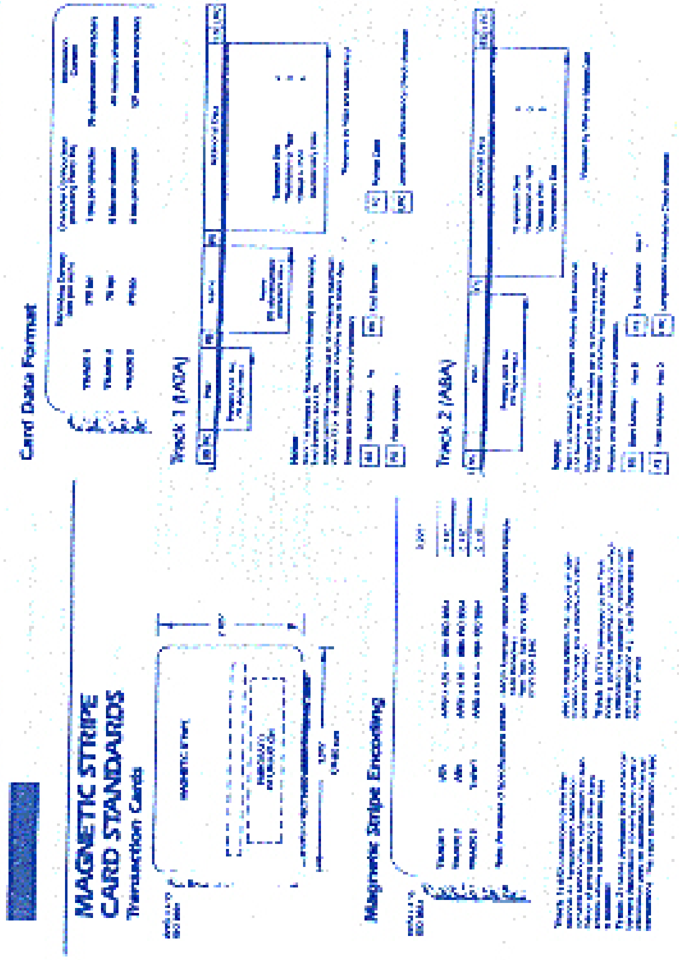
In this section, we will describe several data formats which are used in credit cards. We will only describe the three tracks as they were described by ISO. On the third track a large quantity of formats are used. Only two of them are published here. The real formats as they are used by banks tend to differ from the original ISO standards but a little bit of research can do miracles on these occasions. You might wonder how the bits as described later are encoded onto the card because the schematic as we described above is only capable of putting 180 degree magnetic field changes onto the card. To explain that we use track 2 because the bits are physically the largest and this ought to work with homemade electronics.

Track 2

The bits are encoded as follows: they are separated by reversing the magnetic field. These reversals make the output of your reader go from one to zero or vice versa. Beware: the fact of whether or not it's a one or a zero is not important, but the change in polarity is important. And now, to make it even more complicated, not only is there a magnetic reversal between two bits but also in the middle of a binary one is a reversal. So if you have a constant moving head over your card, software should be able to determine whether they are reading a zero or a one. In fact, nobody is capable of speeding up the speed of his reading head twice within the time period of one bit. Therefore, even a constant speed is not required. So you will get away with cheap, lousy equipment.

Now you have a whole lot of ones and zeroes inside your computer and still you don't know anything. The important thing here is to know the bit stream starts at the left side of the card so the strip is being read from right to left and after a couple of zeroes the data will start in the following format: P1248P1248 etc.

The P stands for parity bit and the 1,2,4,8 stand for the decimal values that they represent (0001 0010 0100 1000). If you decode this, there is your data, which is similar to the Track 2 specifications (ABA). How the LRC character works (a checksum) we don't know yet. But our mailbox is open to any suggestions.



MAGNETIC STRIPE CARD STANDARDS

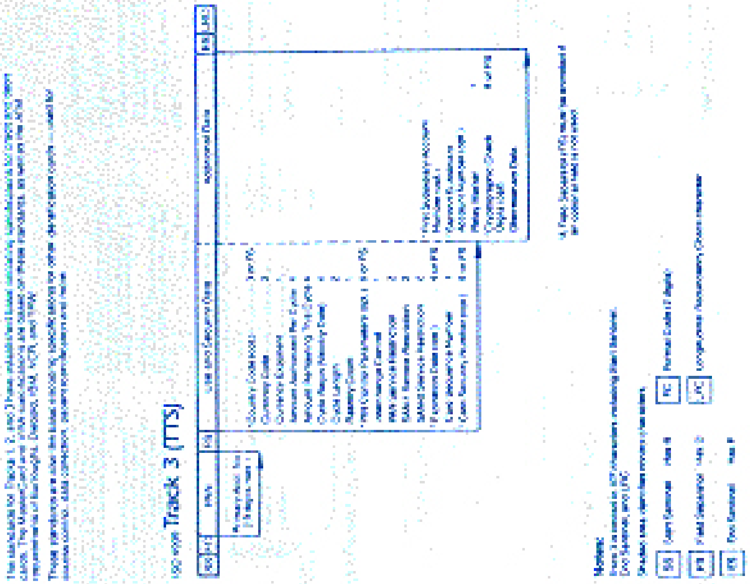
Transaction Cards

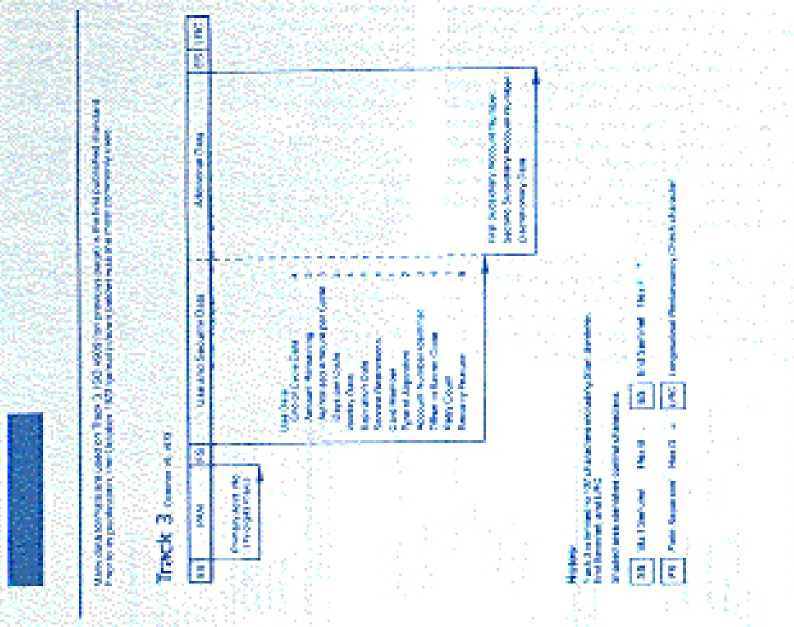
Magnetic Stripe Encoding

Card Data Format

Track 1 (IATA)

Track 2 (ABA)





Plastic Cards - Embossing/Encoding Systems - Service Bureau

death of nynex business centers

by Anonymous

On June 1, 1991 NYNEX Business Centers sold its entire operation, assets, and customer base to rival computer reseller ComputerLand.

The five-year experiment was the most serious attempt yet by a Bell Operating Company to capture the long-predicted home and business markets for new synergistic computer/communications technology products, such as desktop computers, modems, integrated voice/data terminals, videotext, ISDN equipment, CLASS hardware, multimedia, facsimile, cellular, and more. In the end though, under a blanket of bureaucratic mismanagement and miscalculations, the division failed to meet its five-year profit plan and was sold to the highest bidder for $125 million in cash and ComputerLand stock, leaving some NYNEX employees either without work or with a company whose name sounds like an amusement park.

I worked for NBC (as it was referred to internally) for the last four of its five years, and I found it interesting to see the telephone giant from the inside. NBC was a division of BISC, the Business Information Systems Corporation division (which also owns the CASE software giant AGS), which itself is part of a still larger division that controls their other "unregulated" companies such as NYNEX Mobile Telephone. It was a confusing hierarchy of divisions and subdivisions which seemed to change as frequently as the seasons (or managers). Although the $25 billion NYNEX Corporation has repeatedly denied allegations that it subsidized its unregulated businesses with the billions in revenues from New York Telephone, many NBC employees (including myself) felt like they were part of a huge, mysterious shell game. In fact, NYNEX is currently under investigation by the Public Service Commission for questionable transactions between the telephone company and its subsidiaries.

For a brief history, NYNEX Business Centers was itself born out of the ashes of two other failing computer ventures. Back in 1986, IBM's chain of retail microcomputer stores (known as IBM Product Centers) wasn't performing up to Big Blue's expectations, so they put it on the block with the stipulation that all employees be retained. NYNEX took the bait, and also bought the failing DATAGO computer chain at about the same time, eventually building a distribution network employing nearly 2000 people in over 80 stores with locations in most states. The nerve center (with an IBM 3090), headquarters, and warehousing facilities were built in Atlanta for its central location, tax laws, and its proximity to major air transport facilities.

This was barely two years after the great AT&T breakup/divestiture that allowed Bell Operating Companies (BOC's) to compete more freely and market non-telephone products and services. At the time, NYNEX was (and still is) employing its Washington lobbyists and PR army in an attempt to convince the U.S. Justice Department to overturn the Modified Final Judgement (MFJ) that forbids BOC's from developing, manufacturing, and marketing their own equipment, and from developing and marketing information services (such as business and consumer databases, electronic yellow pages, etc.).

Evidently though, the Reagan administration was having such a ball deregulating the S&L industry that they never got around to cutting the ribbon on any new parties. So, NBC was limited to reselling only other manufacturers' products (such as IBM, Compaq, Apple, Hewlett-Packard, etc.) in a highly competitive market they never could hack. NYNEX kept up the deregulatory fight though, urging its employees to write their legislators to deregulate BOC's in an unprecedented, self-labeled "grass roots" campaign which never bore fruit. It's almost certain to happen eventually because there's billions of dollars at stake, but it's too late for NYNEX Business Centers.

HACKER NEWS

On June 12th, Len Rose (whose story was featured in our Spring issue) was sentenced to a year in prison for sending AT&T UNIX source code over the telephone.

To further intensify the witchhunt atmosphere of this charade, the judge (U.S. District Judge J. Frederick Motz) ordered Rose to sell his computer equipment.

This is certainly one of the stiffest sentences ever handed down in the hacker world, no doubt to send another message to us all. (In fact, Rose could have been ordered to pay restitution to AT&T, presumably for the trauma of having to charge him with this crime.) What's particularly crazy here is that nobody is saying that Rose ever broke into a system or even did anything with the source code, other than examine it. Basically, Rose got ahold of something AT&T didn't want him to see, so be was put away for a year. If the case has to be summed up in one sentence, that would certainly suffice. We'd like to know how many people are comfortable with a system that locks people away for just looking at programs and experimenting with them in the confines of their own home. How many of you could resist a glance at UNIX source code if you were capable of understanding it and if it happened to be within your grasp? It's human nature to be curious. For ages, we've been punishing and suppressing human nature in various ways. But it never seems to work because human nature has this way of bouncing back and surviving. Hackers epitomize this and will also never disappear. But they may be forced into hiding for some time to come, something that will set technology back significantly.

For those interested in writing to Len Rose, his address is: Federal Prison Camp, Seymour Johnson AFB, Caller Box 8004, Goldsboro, NC 27531-5000.

***

While some hackers are going to jail, others are trying to sell their talents. Former members of the Legion of Doom have teamed up to start Comsec Data Security in Houston.

Former hackers Erik Bloodaxe, Doc Holiday, and Malefactor started the organization this summer. "People need us," said Holiday, whose real name is Scott Chasin. "We're the best. Ten years from now we'll be the leaders in data security."

According to Comsec's press release, "We feel that we are bringing a fresh approach to security consulting in the corporate marketplace. We were all the cream of the crop of the computer underground and know precisely how systems are compromised and what actions to take to secure them."

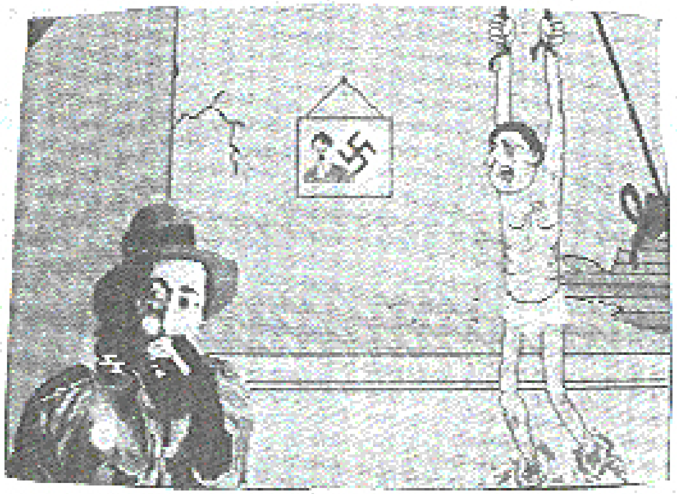
The group estimates its success rate at penetrating systems to be 80 to 85 percent.

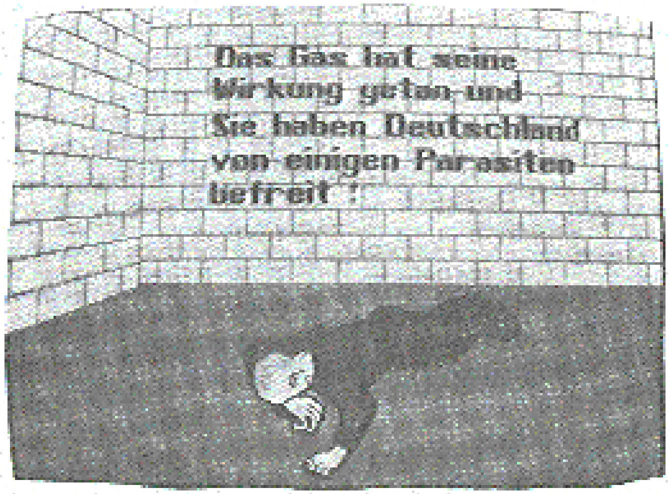
Many in the corporate world say, at least publicly, that they would never trust former hackers to do security for them. Those still in the hacker world tend to look upon Comsec with a mixture of suspicion and contempt. We will reserve any judgement until we see just what it is they do and how good they are. We do hope, however, to see them try educating their clients on just what a hacker is, even though fueling the current paranoia would make them much richer.

Comsec can be reached at 713-721-6500. (Except for the area code, that number is *real* similar to ours!)

From: len@netsys.NETSYS.COM (Len Rose)
Newsgroups: comp.dcom.telecom
Subject: Farewell
Message-ID: <telecom11.481.7@eecs.nwu.edu>
Date: 21 Jun 91 23:27:01 GMT
Just a quick note to say Goodbye to many friends and compatriots.
I will be off the net for about a year I suppose. Many of you deserve
more than just "Thanks" and some of you deserve utter contempt.
Watch yourselves. It can happen to anyone.
Len

JEW-DISM





Got your attention, didn't it? These are pictures from a neo-Nazi computer game circulating throughout Germany. One picture depicts a Gestapo agent torturing a prisoner. The other is a congratulatory message: "The gas has taken effect and you have freed Germany of these parasites." One group fighting against this kind of thing is the Simon Wiesenthal Center, 9760 W. Pico Blvd., Los Angeles, CA 90035.

Build A Tone Tracer

by Mr. Upsetter

If you have ever browsed through catalogs of telecommunications equipment, you have probably seen a device called a "tone tracer". These little devices cost around $30 and are used by telco linepersons. The main function of a tone tracer is to place a tone on a telephone cable pair so the pair can be physically tracked or easily identified when in a large cable bundle. A tone tracer also can be used to check the polarity of a phone line, roughly measure continuity, and provide "talk power". You can build your own tone tracer from a handful of parts for just a few dollars.

Circuit Description and Operation

Please refer to the schematic diagram. The circuitry basically consists of two parts: a tone generator and an amplifier. The tone generator can generate either a steady tone or a warble tone. NOR gates IC1c and IC1d along with C2, C3, R2, R3, and R4 create the tone. Gates IC1a and IC1b are used to switch between steady and warble tones. C1 and R1 control the rate of the warble tone. The frequency of the steady and warble tones is controlled by C2, C3, R2, R3, and R4. Q1 and Q2 form a push-pull amplifier whose tone output is capacitively coupled the phone line by C4.

When switch S2 is set to TONE, the 9V battery powers the tone generating and amplifier circuitry. If the tone tracer is connected to a speaker or a phone line, a loud tone will be heard. When S1 is set high, there will be a steady tone. When S1 is set low there will be a warble tone.

When S2 is set to CONT, the 9V battery is connected to D1, R7, and R8. The device now functions as a basic continuity checker. The brightness of the LED will vary with the resistance that is connected across the tone tracer. Also, when connected to a phone line, the tone tracer now provides talk power. If the phone line is completely dead (there is no voltage whatsoever on the line), then the tone tracer will provide enough voltage to power a couple of lineman's handsets or basic phones. This way communications can take place over short distances.

When S2 is in its center (off) position, the battery does not power the circuit at all. However, when the tone tracer is connected to a phone line, R7, D1, and R8 are connected across the phone line. Now the polarity of the line can be checked. If the alligator clip marked RING is connected to the ring (-48V) side of the line, and the alligator clip marked TIP is connected to the tip (ground) side of the line, the LED will light. If the clips are reversed, the LED will not light. Typically, the tip wire is green and the ring wire is red.

Also, note that when connected with the correct polarity, the LED will be bright when the line is on-hook and dim when off-hook. When a ringing signal is present, the LED will flash.

Construction, Testing, and Tracing

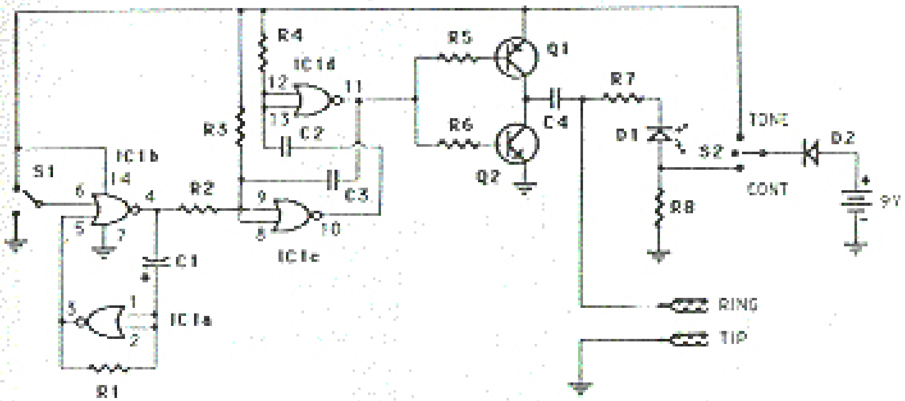
Construction of the tone tracer is fairly straightforward and doesn't require any specific layout. You will probably want to solder it together on a small breadboard so it can be built into a compact, handheld enclosure. For convenience, you may want to connect a phone plug as well as alligator clips to the output of the tone tracer. Also, you may want to use a socket for the IC. All parts are available from Mouser Electronics. Call 800-246-6873 to get your free catalog.

After you have constructed your unit and double checked all the connections, connect it to a small speaker and switch S2 into the TONE position. You should hear a rather obnoxious tone. Toggle S1 to make sure you get both warble and steady tones. Then disconnect the speaker, connect the tone tracer to a phone line, lift your phone off hook, and do the same thing. The other minor functions should be easy for you to check out on your own.

Tone tracers are designed to be used with an inductive pickup of some sort. Inductive tracing is advantageous because no physical connections need to be made to the line, thus no wires need to be cut, no clips need to be hooked onto terminals, etc. It makes the job quicker and simpler. To trace the tone of our tone tracer, you could spend $40-60 on a "line probe" type inductive pickup designed for the purpose. But since you went out and built your own tone tracer from scratch in the first place, you probably don't want to do that. A marginal alternative is to use a basic audio amplifier (such as Radio Shack 277-1008) and a suction cup pickup (Radio Shack 44-533). Connect the tone tracer to a phone line and switch S2 to TONE. You will be able to hear the tone when the pickup is placed very close to the cable or its terminal block. Winding 1 or 2 turns of the cable around the pickup should improve things. Unfortunately, this setup is vulnerable to 60 Hz noise from electrical wiring. You will need to rotate the pickup for the least amount of buzzing.

Parting Words

A tone tracer is a handy thing to have at times. So instead of shelling out some cash to Specialized Products or Jensen Tools, you can build this simple, cheap circuit. But for those of you who are not electronically inclined, there is an even easier and cheaper way. In most areas, there is a test number you can dial that puts a loud 1004 Hz tone on your line. For instance, in certain parts of California this number is your prefix plus 0002. Of course, you need to know the test number in your area to take advantage of this.



PARTS LIST:

C1- .47µF electrolytic
C2, C3- .01 µF monolithic 20%
C4- .1 µF 100V
D1- standard LED
D2- 1N4004
IC1- 4001 CMOS quad NOR
Q1- MPSA92 PNP
Q2- MPSA42 NPN

R1- 1M 1/4 W
R2- 470K 1/4W
R3, R4, R5, R6- 100K 1/4W
R7- 1K 1/4W
R8- 8.2K 1/2W
S1- SPDT
S2- ON-OFF-ON

Additional parts: large alligator clips, modular phone plug, 9V battery and clip, IC socket, enclosure, PCB.

TONE TRACER SCHEMATIC DIAGRAM AND PARTS LIST

hacking mcimax

by MCI Mouse

MCIMAX is actually MCI's link into the MAX database which contains information concerning many MCI as well as AT&T and US Sprint products. The data retrievable for each service includes current usage rates and volume discounts for products, comparison matrices, feature and benefit statements for products, guidelines for entering and processing orders, and current product promotions.

This article will deal specifically with MCIMAX, containing information about MCI's domestic products.

MCIMAX can be logged into from an MCI terminal. I am writing this article under the assumption that you can access the MCIMAX database remotely either via dial-up or network hopping. From an MCI Terminal ID Screen, type L PREF (for Mid-Atlantic, Northeast, Southeast, or International divisions) or L PREFSAC (for Midwest, Pacific, Southwest, or West divisions). At this point, you will be prompted for a Sign-On Number, Volume Name, and Password. For Sign-In Number, enter R### where ### is the branch ID number. The branch IDs go by hundreds (for example, 500 to 536 is the Southwest Division range). Your volume name is MCIMAX and a password is not required at this time to access the database. You should now be in the MCIMAX database.

MCIMAX is structured like a book. There are 26 chapters, A through Z, containing the following information:

A Reserved
B Dial "1"/Premier Calling Plans
C Operator Services
D Corporate Account Services/CAS PLUS
E WATS
F Hotel WATS
G University WATS
H PRISM I
I PRISM II
J PRISM III
K PRISM PLUS
L MCI 800 Service
M Vnet
N Fax
O MCI Card
P Worldwide Direct Dialing
Q Digital Gateway T-1 Access
R Fractional T-1/DSO and VGPL
S Terrestrial Digital Service 1.5
T Digital Data Service (DDS)
U Switched 56 Kbps Service
V Hospitality Plus
W MCI Network
X Rate Tables
Y AT&T Competing Products
Z US Sprint Competing Products

Within each chapter, there are topics, sections, and items (i.e. in Chapter K, PRISM PLUS, Topic 1 is Description, and sections include Description Introduction, Overview, Call Processing, Target Market, and Sales Successes). The bottom of your screen should contain the pertinent information as to how to select your sections within the topics of a chapter, but if not, you should place an X by the section which you wish to browse.

Another way of accessing information is via the Index. From your arrow prompt at the bottom of your screen, you can type an Index word or a letter if you're not sure of the exact index entry. For access to AT&T 800 Readyline rates, for example, you would type ATT 800 READYLINE, RATES. If you simply typed A, you would be given an alphabetical list of topics within the Index from which to choose. Tab moves from item to item from the list, and an X by the topic will go to that Index item.

Function keys to use with these menus include:

#* PF1 Displays previous page/topic.

#* PF2 Displays next page/topic.

#* PF3 Exits to MIS logo screen.

* PF4 Displays table of contents.

#* PF5 Lists the chapters in the volume.

#* PF6 Lists the topics in the chapter/volume.

* PF7 Lists the sections in the topic.

#* PF8 Allows you to type an index entry/displays the index.

PF9 Displays the previous chapter in the volume.

PF10 Displays the next chapter in the volume.

#* PF11 Gives access to bookmark or glossary options/shows more options.

PF12 Toggles the menu (at the bottom of the screen) on and off.

(A # indicates use with Table of Contents and a * indicates use with the Index.)

The bookmark function allows you to return to a set screen at any time. Using the PF11 key to see the options, hit PF9 to set the bookmark. Then enter a name for the bookmark when asked. To go back to where you were, hit PF11 again. From the PF11 menu, you can retrieve a bookmark by entering PF10 and choosing the name of the bookmark to return to.

There is also a glossary available in MCIMAX. If the bottom of the screen's display does not have PF8 indicated as "Glossary", hit PF11 to toggle. Once selecting PF8, use the PF1 key to get a list of glossary terms, and enter the term to be defined at the prompt, or enter a blank line to return to your previous work.

Although this system is not as intriguing as some telecommunications computer systems, it is good to know what you're toying around with if you stumble upon one. Good luck and have fun!

Inspect Implementation

We received an internal document recently concerning security implementations on Digital's EASYnet. The employee who supplied this information wishes to be known as Condor Woodstein. We will quote some of the more interesting sections.

"Someone has written that 'failing to plan is planning to fail.' No where [sic] could this be more true than in the area of security. In an effort to improve upon our planning, a new security tool is being released for all VMS systems. This tool will run with SECURPAK, and will provide the system manager with a new level of system security testing that was never before available. Additionally, it will complete the process by providing a greater level of reporting than exists today.

"...INSPECT will be required on all VMS nodes of the EASYnet. INSPECT, Interactive Network Security Policy Examination/Compliance Toolset, has been developed to meet the rigors of Corporate Security Standard 11.1. When run, INSPECT will check a system to ensure that it is in compliance with this security standard.

"All system managers in DECNET Areas 16, 34, and 36 are being asked to install the INSPECT tool on their system by December 30, 1990. Additionally, any system manager of a system in a hidden area, ie: 62, 63, who is serviced by an area 16, 34, or 36 pass-thru server must also install INSPECT. INSPECT is now a required security tool, just as SECURPAK is. The XSAFE security testing tool now tests for the existence of INSPECT on your node.

"...Presently, Digital Equipment Corporation owns the 'largest proprietary computer network in the world.' This network, EASYnet, is a target for hackers, and others. The EASYnet represents a wealth of resource that is available to the Digital employee, and it is a resource that must be protected. INSPECT is a tool that will assist the system manager in safe guarding [sic] our resources.

"INSPECT is divided into two portions, inspectors and agents. Basically, inspectors are assigned a specific task. Agents are generated by the inspectors, and carry out the actual investigation. INSPECT's purpose is to check the security of your node, in an ongoing manner, and review 5 major subsystems on your system. They are:

"File Subsystem: system file ownership and protections, overall file protection, public and private, world writeable [sic] files.

"Account Subsystem: checks for privileged accounts, account ownership, proxies, system support accounts, and inactive accounts.

"Network Subsystem: checks network objects, DECnet access, Dialup and LAT protection.

"SYSGEN Subsystem: compares SYSGEN parameters for changes.

"Audit Subsystem: checks for security auditing and OPCOM.

"At a minimum, INSPECT runs automatically every 28 days, and reports the findings of these subsystems to the Security Office, as well as generates a report to be used by the system manager. This report can be used to correct potential security 'holes'.

"Furthermore, INSPECT can be run on demand by the system manager, and it is encouraged that INSPECT be run whenever there is a change made to a system, whenever unaccountable changes are found, or whenever increased activity is noticed on your system.

"...INSPECT provides reporting capabilities to both the system manager and the Security Office. As INSPECT finds potential security issues, it attempts to resolve them by creating a DCL command procedure that will 'patch the hole.' INSPECT does not apply the patch that is developed. It is up to the discretion of the individual system manager to ensure that this is performed. It becomes part of the system manager's responsibility to check for VAXmail messages from INSPECT, and take corrective action if necessary.

"Information regarding LOCKDOWN is being provided to the system manager to ensure that they understand what LOCKDOWN is and what it does. Until otherwise notified. *** LOCKDOWN SHOULD NOT BE UTILIZED ON ANY SYSTEMS **

"Perhaps one of the most misunderstood features of INSPECT is LOCKDOWN. LOCKDOWN is a default feature of INSPECT. Whenever INSPECT is run, it creates a file in the SYS$MANAGER directory. This file is named: "SYS$MANAGER:INSPECT$node-name_LOCKDOWN.COM

"This file contains DCL code for each violation that INSPECT finds, and is readable by the system manager. INSPECT does *not* process this file, or apply any patch to your system. At the end of an INSPECTion, a VAXmail is sent to the system manager for review. The VAXmail contains all the security issues that INSPECT found. INSPECT also notifies the Security Office of the node violations by sending a token of information. This information is automatically placed in the Regional node database.

"...LOCKDOWN is run interactively, and 'suggests' values or options for the system manager to use. The system manager is always prompted to determine if a change should be made, and the LOCKDOWN procedure does not make any changes without first consulting the system manager. This is key to the understanding of LOCKDOWN. INSPECT will not change anything that you do not approve. When used in this manner, the system manager will find LOCKDOWN to be very helpful as all the necessary commands to correct a security issue have already been set up. All the system manager has to do is approve the processing of them. By regularly running INSPECT, and reviewing the LOCKDOWN file, the system manager will become familiar with what needs to be done, and should find the LOCKDOWN feature helpful.

"On a test Micro-VAX, with only 8 accounts, INSPECT generated a 75 block command file of DCL code. Larger systems and clusters will generate a much larger file. System managers are encouraged to carefully read and utilize this code. Some of the items that the LOCKDOWN code can do for you by default are:

"Ensure that all non-privilege accounts have a password minimum of 8 characters.

"Ensure that privilege accounts have a password minimum of 15 characters.

"Delete SYSUAF entries for SYSTEST, SYSTEST_CLIG, and FIELD.

"Modify SYSGEN LGI (login parameters).

"Ensure that all accounts expire.

"Enables VMS Accounting and AUDIT.

"Set protections and ACL's on files in accordance with standard 11.1.

"Rename the DECnet SYSUAF entry to DECnet$SERV.

"...As indicated in the INSPECT v2 installation, the system manager is cautioned against blindly running the LOCKDOWN procedure. Careful evaluation of the procedure's contents is encouraged. It is possible that the LOCKDOWN procedure may effect other layered products on your system. For example, LOCKDOWN inserts commands to start VMS accounting. If you are running on a smaller VAX, ie: Micro-Vax or a 3100, you probably have 'lean' disk space, and probably don't want ACCOUNTING running. In this case, when you are prompted by LOCKDOWN regarding the running of VMS ACCOUNTING, you would use the default, 'N'. In this case, LOCKDOWN would not start accounting.

"...Every 28 days, at minimum, INSPECT will check your system and send a token to the 'Security Office.' The Security Office is a special node that is set up to receive these tokens of information and process them. Within Central States Region, a node is being set up that will be the focal point for INSPECT tokens. The Security Office will be able to track nodes throughout the Region, and ultimately Corporate Security will be able to track the entire EASYnet. Nodes suspected of being open to intrusion will be contacted and required to take corrective measure.

"Perhaps one of the more important features of the Security Office is its ability to generate mail messages. Security managers will be able to review the results of the INSPECT tests quicker, and can utilize the automated features of the Office to mail discrepancies to both the System Manager and the cost center manager. The office can generate 3 types of canned reports:

"1. A report of all nodes that have issues.

"2. Generate VAXmails directly to system managers, with a copy to the cost center manager, for every node that has an issue.

"3. Generate mail memos sent directly to System Managers, with a copy to the cost center manager for 'Missing Tokens'. This memo indicates that INSPECT either is not running on your node, or has not been installed.

"Agents are generated by the inspectors, and carry out the actual investigation."

"...INSPECT will be used in conjunction with XSAFE. In fact, XSAFE now checks for the installation of INSPECT on your node. Any node that does not have INSPECT installed will be flagged by XSAFE as a violation.

"For those who may not be aware, XSAFE is an external tool used by Corporate Security to test every node on the EASYnet each quarter. XSAFE actually attempts to break into a node by logging into known accounts that should be turned off. It checks file privileges on system and network files, and performs other security tests. At the end of the test, the results are VAXmailed to the SYSTEM account where the system manager can read it and correct the issues. Additionally, the results are sent to the master XSAFE database. Quarterly, a report is generated showing the results of all XSAFE testing in the geography. Nodes which contain failures are contacted and requested to address the violation.

"...Hidden areas are actually 'small or local' DECnet areas within larger DECnet areas, and are used to place additional nodes on the network when network space becomes scarce. A single large DECnet area may have many, smaller hidden areas. The hidden area is separate from the EASYnet, but connected via a pass-through server. This server allows the hidden area users to access systems and data much as any other system, except they must pass-through the server to get to it.

"When installing INSPECT, systems in a hidden area should consider their Security Office to be their pass-through server. That is, the system that connects their hidden area to the EASYnet serves as the Security Office for that hidden area. When INSPECT is installed, merely point it to the pass-through server. System managers responsible for pass-through servers will need to install INSPECT indicating that this node is a pass-through server. This indicates that the server will need to take the INSPECT token it receives and pass it to the Central States Security Office node.

"...All EASYnet nodes must continue to run SECURPAK. Nothing changes with regard to this utility. All system managers should have SECURPAK installed and running on their respective nodes, and should be reviewing the reports generated by this tool. In comparison, SECURPAK runs each daily and delivers reports to the system manager. SECURPAK looks a [sic] login failures, and other items as selected by the system manager. INSPECT, on the other hand, does not run daily, it runs as scheduled by the system manager. INSPECT digs deeper into the system, and communicates its findings to the Security Office, SECURPAK doesn't. These two tools, when combined, will make it easier for the system manager to ensure that their system is secure.

"...Any time that you suspect that your system, or the EASYnet has been compromised, do the following:

"A. Use the VMS AUDIT command to dump the audit log: $ANAL/AUDIT/SINCE=DATE/OUTPUT=filename SYS$MANAGER:

"B. Mail this log electronically to ANCHOR::NETWORK. Include you [sic] name, address, and DTN.

"C. Call Network Operations and inform them of your situation.

"D. Call Central States Regional Security.

"E. Keep communication with regard to the incident within a close circle of individuals. Do not spread information regarding the incident that may or may not be true. You might not have a problem.

"...System managers now have both SECURPAK and INSPECT to use in securing their systems, as well as VMS Security features such as AUDIT. When combined with the external testing of XSAFE, the EASYnet will become a much more difficult target for hackers to penetrate."

the class struggle

We have obtained internal documents from Bellcore which go into some detail on CLASS services that are being offered around the country. Because these services are of growing concern to our readers and much of the population, we will share this information here.

Caller ID is referred to here as Calling Number Delivery (CND), "a revenue-producing service intended for residential and business telephone customers.

"...When CND is activated on a line, the DNs [directory numbers] of terminating calls are transmitted to the called CPE [customer premises equipment]. For an interoffice call [calls between two different central offices], the caller's DN is transmitted from the originating Stored Program Controlled System (SPCS) to which the calling party is connected, to the terminating SPCS to which the called party is connected during call setup. It is then transmitted from the terminating SPCS to the CPE during the first long silent interval of the ringing cycle [between the first and second rings]. A long silent interval is defined as an interval of silence lasting 3 or more seconds. For an intraoffice call [calls within the same central office], the caller's DN is retrieved from SPCS memory for transmission to the CPE. Then, depending on the options offered by the CPE, the DN is displayed and/or printed out. The CPE might also be arranged to store the DN for later retrieval by the customer. These options are transparent to the SPCS, i.e., the SPCS performs the same actions for each case. For both interoffice and intraoffice calls, transmission of CND data from the terminating SPCS to the CPE should *never* take place while the CND customer is in an off-hook state.

"Finally, CND service allows the called CPE to receive a 4-digit or longer Personal Identification Number (PIN) instead of the calling DN. The PIN would be dialed by the calling party as part of the calling sequence. Receiving a PIN would indicate that the call is from someone that the called party probably wants to talk to, even though the call might be from a line having a DN that would not have been recognized if displayed to the called party (e.g., a coin line).

"In each of these cases, the data transmission is provided via a simplex voiceband digital interface (VDI). Requirements for this interface are defined in TR-TSY-000030, *SPCS/Customer Premises Equipment Data Interface.*

"...Although not offered initially, it might be desirable in the future to provide an interface to Directory Assistance or another database so that the calling party name instead of the calling DN can be determined and transmitted to the called party's CPE for display.

"...If possible, an attempt should be made to retrieve a partial calling line DN (e.g., less than seven digits for intraNPA calls, less than ten digits for interNPA calls) if the complete DN is not available due to a lack of Common Channel Signaling (CCS) connectivity. If a partial DN is determined, it should be transmitted to the CPE. The NPA portion of a partial DN should always be included in the transmission to the CND customer's CPE, even if the call is intraNPA. If neither a partial DN nor a complete DN is available, an out-of-area/DN-unavailable (O/U) indicator, signified by the letter 'O', should be transmitted to the customer.

"The following describes responses to irregular user action during activation of CND.

"The customer may dial an incomplete, nonexistent, or erroneous feature activation or deactivation code when attempting to enable or disable this service. If the activation or deactivation code dialed for CND is incomplete or nonexistent, the customer should, as a minimum, be given reorder tone. However, it is desirable in this case to give the customer a voice announcement explaining the situation encountered. If the dialed code exists but is not the correct code for the service, another service may be inadvertently accessed. This would occur if the customer's line is allowed access to the service associated with the dialed code. To lessen this problem, customers attempting to access the CND service should be given a voice announcement verifying that the service has actually been accessed.

"If a CND activation or deactivation code is dialed by a subscription customer, then reorder tone should be given.

"Similarly, when dialing the activation or deactivation codes for CND, the customer may also request activation of the service while the service is already active, or request deactivation when the service was previously disabled. In these cases, it is desirable to provide an announcement explaining to the customer that the service was already activated or deactivated, as the situation requires. If this is not feasible, the customer should be given a confirmation tone.

"...The allowable data transmission rates for this service are given in TR-TSY-000030. It is desirable that a rate of 1200 to 1800 bits per second be provided for this service.

"...CND uses CCS [Common Channel Signaling] to transmit the calling line DN from the originating SPCS to the terminating SPCS. The protocol used by this feature should be Signaling System Number 7 (SS7), as specified in TR-NPL-000246, *Bell Communications Research Specification of Signaling System No. 7.* This feature should be capable of functioning on an intraoffice basis if the office is not served by a CCS network.

"Originating offices equipped with SS7 should include the calling DN in the address information field within the calling party address parameter of the Initial Address Message (IAM) for all BOC [Bell Operating Companies] and intraLATA interoffice calls placed over trunks served by SS7. In addition, if the calling party address is a private number or is a DN from a line having the calling number privacy feature active, the presentation indicator field in the Calling Party Number Parameter of the IAM should be set to '0 1' (i.e., 'presentation restricted'). A terminating office should expect to find the calling party address in the IAM if the intraLATA call setup path does not involve an interexchange carrier and is served entirely by SS7. TR-TSY-000317, *Switching System Requirements for Call Control Using the Integrated Services Digital Network User Part (ISDNUP)* states that the calling DN is a required field in the IAM.

"...CND is not available on operator-handled calls.

"...Special customer-initiated testing does not have to be provided; the customer is normally able to determine if this service is operating correctly when an incoming call is received. However, it is a desirable option to allocate a DN within each SPCS equipped for CND (the DN to be specified by the telco) that the customer can dial to receive a sequence of test data messages. This gives the customer a more positive testing mechanism and can prevent some customer trouble reports. If this customer testing capability is to be provided, the customer should be able to dial the special DN, hang up, and receive a series of test data transmissions designed to check the capability of transmitting any digit in each position. The first test message should begin within 10 seconds of the customer disconnect and should contain the pattern '0123456789'. The remaining nine messages should rotate each of the digits (0 through 9) in each of the digit positions. Two additional test messages should transmit the letters 'P' and 'O', respectively."

All of this only scratches the surface. There will be many more details to reveal. You can obtain a free listing of Bellcore documents by calling 800-521-CORE and asking for document SR-TSY-000264.

Caller ID decoders are now available to hackers in kit form. International Micropower Corporation (800-992-3511) sells the IMC-CID-1K for $38. It decodes the Caller ID datastream and converts it to the RS232C serial format. MS-DOS software is available for $6.50 that displays and logs all data to disk. The unit (also available assembled for $45.50) is much less expensive and similar to commercial PC-compatible Caller ID decoders costing hundreds of dollars. This device allows you to actually study the actual binary datastream.

The Letters Section

UNIX Password Hacker

Dear 2600:

I looked at the source for the UNIX password hacker in the latest issue, and it's bogus. Not that it won't work. It probably does, but it's conspicuous as all hell on most systems.

Let me explain. It calls crypt(3), right? That's a system call, and most UNIX boxes log system calls for various accounting reasons. But crypt(3) is special. A lot of boxes are set up so that if something starts calling crypt left and right (like the program you published), red lights go off. At the very least, it's going to give the pathname of the program calling crypt all the time.

And running strings(1) over the binary, even if the source has been deleted, will show that it involves crypt, */usr/dict/words*, and even newsrc.

Let me say why this is important. If you've been reading usenet, sysadmins don't slap you on the wrist anymore, once they find you're running a password hacker. Someone at University of Georgia's just been suspended for mailing out the */etc/passwd* file to someone else. He was just a dweeb who helped a hacker. Suspended. I'd be really upset if it were me.

Here's what might be done instead for dealing with passwords. 1) Get sources for something which works just like crypt(3). 2) Upload these, */usr/dict/words* (or something like it), and */etc/passwd* to your PC. Security is a two way street. Don't use a public system for stuff you don't want others to know about. 3) Run a version of your password hacker locally. It's a little slower, but you can't get nailed for it.

(Or you could just grab the source for COPS, and run it locally. It does the same thing.)

rj

Dear 2600:

I have read three issues of your magazine and I am impressed. As a system administrator of eight UNIX systems, I find the information about hacking to be useful in keeping my systems secure (I am currently re-writing the UNIX password hacker to examine all the passwords on my systems and e-mail the users who have "hackable" passwords.)

I feel that your publication is necessary to help drive home the point that computers are simply another method of communicating and that the founding fathers protected our right to communicate in the First Amendment. And further, that a legitimate government of the people should have no fear that the individuals that make up the population can communicate. While you guys are not as polished as the EFF, your message is a solid and strong one. Further, even if I did not agree with your message (and there are some parts of it that I feel promote theft of services, which I disagree with), I believe that you have a First Amendment right to publish things that I do not agree with.

All in all, I am glad to have subscribed to your magazine and I look forward to receiving future editions.

DP

Dear 2600:

Thanks for a great magazine! I just started picking up your magazine a few issues back and I'm more and more impressed with each issue. Your article about the UNIX password hacker was fantastic. So far, I've been able to run it without any modifications on BSD, Ultrix, and AT&T UNIX System V systems and it worked perfectly every time, giving me passwords to more accounts than I could ever need. But I hope you don't mind if I make a suggestion. On one system I was running Uhacker on, the system administrator was really poking around with my compiled program and it made me pretty nervous. Since Uhacker automatically goes into the background, why not just go ahead and delete it once it's running? That way, no one can screw around with it. You'll have to recompile to run it again, but it's a lot safer to do it this way. Thanks!

NEXUS 6

Unfortunately, a nosy system administrator is likely to kill background processes (s)he doesn't understand. By far the best method is to employ a program that runs on your own computer and interacts with a downloaded password file. This cannot be interfered with and is not illegal in any way - the law is only broken if you use (or attempt to use in some cases) somebody else's account without permission. Figuring out their password is not the same thing.

Another 2600 Meeting

Dear 2600:

Please notify other 2600 subscribers in Arizona of our decision to have the first Arizona 2600 meetings with the Phoenix ICCA (independent computer consultants) meetings. Several members of the Phoenix chapter of ICCA are also subscribers to 2600. Our meetings are normally the second Tuesday of each month. Times are: happy hour: 6:00 pm., dinner: 7:00 pm., meeting: 8:00 pm. We meet at the Executive Park Hotel, 1100 N. Central Avenue in Phoenix. The Phoenix ICCA chapter's hotline is (602) 996-2612.

Access From Korea

Dear 2600:

Greetings from the Republic of Korea. I have a question about your Winter 1990 "Word on the Street". You mentioned Sprint's "Sprint Express" service, and some of the countries it served. Do you know if Sprint also serves the ROK? If so, can I reach it on a military phone? USA Direct is 550 HOME for military phones but they won't process 800 numbers so I can't call Sprint's customer service number. Can you help me?

Marooned in the ROK

According to the people at Sprint, South Korea is not on their immediate list. The same is true for MCI's Call USA and Alnet's Option USA. If you need to speak to someone at Sprint, you can try calling 816-854-0903. That's their corporate headquarters in Kansas City. They may even accept a collect call from South Korea. Sprint Express has a bunch of additions since that article appeared. They are: Belgium: 11-0014; Brazil: 000-8016; El Salvador: 191; Finland: 9800-1-0284; Germany: 0130-0013; Ireland: 1-800-55-2001; Israel: 177-102-2727; Italy: 172-1877; Malaysia: 800-0016; New Zealand: 000-999; Portugal: 05017-1-877; Sweden: 020-799-011; and Switzerland: 155-9777.

Red Box Notes

Dear 2600:

In the Spring issue, you published my letter complaining that the red box built from plans published in 2600 (based on the Radio Shack dialer) didn't work. With further experimentation, I have discovered that it does indeed work perfectly only not from NYNEX based phones. From Pacific Bell phones in Los Angeles it works well and in Washington DC it seems to work. I am curious though, as to what ability, if any, the phone companies have in determining which calls were placed with red boxes. It all seems too easy. Keep up the great work you're doing!

Larry
New York, NY

We know of no way specific calls could be flagged as having been placed with a red box unless a live operator suspected something and started an investigation. There are possible scenarios where the phone company could realize that calls to a particular number were being red boxed but, for the most part, the reaction seems to be to replace mechanisms in the payphone itself as NYNEX has done. To this day, though, payphones in the NYNEX region that haven't been serviced in a while (mostly indoors) will still allow red box tones.

Dear 2600:

First of all, being a new member, I'm enjoying the mag.

In reference to the Autumn 1990 issue, page 32-33 - converting a tone dialer into a red box - I made the modification and it has not failed. A great piece of work by somebody.

One thing I found to work and have tested all over California is the local call. I programmed "L1" for a nickel. When I want to call home in town or make any local call, I put a nickel into the payphone, then press L1 three times (calls are 20 cents where I live), then dial the number with no problems. You can't use the unit for the initial five cents.

Anything new as to when California will have Caller ID? The phone company will not say.

TH
Ventura, CA

Some parts will have it before others. But you will get some form of it and probably fairly soon.

UNIX BBS's

Dear 2600:

There are four BBS's that I know of in the New York City area that allow people using personal computers to access UNIX-based systems.

Fordham Jesuit BBS (212-579-2869) has a Netmail section for sending messages to/receiving messages from UNIX-based networks. You are given credits by its sysop and can send a message to anyone as long as you have the exact address of the person to whom the message is addressed (e.g. 2600@well.sf.ca.us). This board is free; there are no monthly charges although a $5 fee and a stamped, self-addressed envelope are requested by the sysop. He'll send you a copy of the rules of etiquette. All registered users get 60 minutes per day. The only annoying feature of the Netmail section is that you can't upload a textfile for transmission; you have to type in the message to be sent.

The Dorsai Embassy (212-431-1944,1948) charges $25/$50 per year for access to UNIX-based boards. Unfortunately, the telephone number is always busy. (The people running this board want to install more phone lines but don't have the money.) It may be a good idea to subscribe as subscribers can use a special telephone number and get more time on the system than those who don't pay anything. There are also two UNIX boards which can be used if you know the UNIX command set and are willing to pay monthly fees.

Mpoint (718-424-4183): this board gives limited privileges to everyone between 11:00 pm and 7:00 am. (If you pay the monthly fee, you can use the board anytime.)

Panix (718-832-1525): similar to Mpoint.

This is probably a very incomplete list of BBS's that access boards run under UNIX. (I only use the *Fordham Jesuit BBS* but have found that the instructions for using Netmail are not very clear.)

There are probably many more boards run under UNIX or providing access to UNIX systems in the 212/718 area codes. I don't know if the general public has access to any of the university systems. I suggest that you call CUNY, Columbia University, etc. for information on public access and fees.

LT

Interfacing With Mainframe

Dear 2600:

We have a database system at work which is linked to a mainframe in another city. This database network deals with inputting and outputting reports concerning equipment via a password. I wonder if you guys or any 2600 readers could tell me how to get into such a system by using my Atari ST and a Supra modem.

MAG
Saudi Arabia

You need to determine whether or not this is a dialup access or a leased line arrangement. If it's the latter, you won't be able to access it from an outside computer or terminal. If it is a dialup, it shouldn't be too difficult to find out the phone number. Since you work there, we *answer you can get, or already have, the password. Now you must get your computer to talk to the mainframe. Is the link high speed or something your modem can handle? If your modem is able to establish a connection (be sure to check parity and stop bit settings), then you have to get the terminal emulation down. That can be accomplished through your modem software once you determine what kind of terminal you need to emulate. (It's possible you won't have to do emulation at all, especially if there are no graphics or screen functions involved.) If all of this goes well, you should be able to do the exact same things on your Atari as you do at work. Just be patient.*

Send A Message

Dear 2600:

I received one of AT&T's "Tele-Gram" letters requesting that I switch to AT&T for my long distance calling.

If you call the number listed on the letter (800-225-7466), you can request to be deleted from AT&T's mailing list. You may also give a reason for your request.

I encourage people to call and request to be deleted. Also request that they take down the reason and inform them of your concern with AT&T's public deception with respect to the Craig Neidorf case and their attempt to make an example of an innocent person.

Dark Overlord

Caller ID Questions

Dear 2600:

I wonder if you could help me with a problem. I get annoying phone calls. Usually they occur on a Monday or Friday. Just about every hour, the phone will ring and a recorded (female) voice says "Please enter your security code" and waits for a four digit touch tone entry. The phone company will not sell Caller ID in our area (Queens, NY). How can I find out who is calling?

Any suggestions, including where I can get plans to build a Caller ID box (if that will work) would be appreciated.

MB

First of all, Caller ID is not in your area yet so a Caller ID box is completely useless to you. Second, Caller ID will not solve your problem unless the call is local. Odds are that it isn't. So you have two options. One is to contact the Annoyance Call Bureau and have them put a trap on your line. If the calls are predictable (same time on a certain day) it will simplify the trace, as will keeping the call going for as long as possible. Your other option is to hack the system that's calling you. You already know it's a four digit code. See if there's any way to get an operator. Try to get the system to do different things. There is also the possibility that somebody is playing a trick on you and connecting you to this machine. If you ever hear a ring before the machine comes on or if it sounds like a three-way connection at any point, that could be what's happening.

Dear 2600:

I'm not sure if you've covered this or not; I'd expect you probably have. Caller ID is the greatest thing to come along since caffeine pills. The Caller ID blocking system they have in my area is bullshit. It will not work if you run the whole gamut of options available. Reason: though the number displays as P or PRIVATE, you can still add the number to your Priority List or call back directly. In which case you can tap your line to see what numbers are being dialed. I haven't tried this; this is an assumption that the numbers are stored in the box, and not in some memory hole in the bowels of C&P. Am I right? If so, don't tell everybody! If the authorities realize this we're screwed.

I also have a question. My home answering machine is the hackable kind that recognizes tones. Something weird, though: at my office we use a phone system with AT&T HFAI-10 phones, and I can't retrieve my messages directly using these phones. It's as if the tones aren't recognized. But if I take another nearby extension, and press the buttons so that the tones on phone #2 come out the earpiece and into the mouthpiece of #1, they're recognized. What would cause this? I know we have standard tones because I can use them for most voice mail applications I've tried (my bank account, etc.). Any comments?

BK
Bethesda, MD

As there are still relatively few areas of the country that have Caller ID up and running, we cannot give you a definite answer. But you should not be able to call a blocked number under any circumstance. That seems pretty logical. If you find that you can, please tell us. The authorities are liable to realize this if it's true - they don't need us to tell them. Regarding your touch tone problems: you probably just have lousy sounding tones. Either they're not loud enough on one particular instrument or they're not long enough. This is a common problem with the newer phone systems. Get a tone dialer (white box) to overcome this no matter where you are. (It's always sad to see technology marching backwards.)

Dear 2600:

Please print a diagram and/or instructions on how to make one of the new Caller ID boxes. Manage that and I'll order all the back issues and a lifetime subscription.

KB
Austin, TX

The call has gone out. Meanwhile check out the August issue of Radio-Electronics. You may also find information to your liking on pages 22, 23, and 41 of the magazine you're currently holding in your hands.

C&P Info Needed

Dear 2600:

First off, the phone number to leave a message for a worker (that includes the First Lady and the President) at the White House is (202) 456-1111. The fax number is (202) 456-2461, also for the White House.

Second thing, to get a computerized voice telling you what number you are dialing from, dial 811. I don't know if this works outside of the Chesapeake and Potomac (C&P) area though.

Finally, I enjoy the hell out of your magazine and it has a great influence in this (the Washington, DC) area - when you published your booklist in the Winter 1990, all the books were checked out at the library, or all sold out at the bookstore, within days of receiving your magazine. Try printing more crap on C&P and a program to "brute force" search all 999,999 phone numbers via modem - to look for modems.

The Monk
Arlington, VA

More Hackerphobia

Dear 2600:

I thought I'd share with you a story, and a tribute to the downward spiral of our society.

I am enclosing a clipping from the course descriptions for my high school. When I read the description for a computer technology course, I said to myself, "Cool, I can finally use my school time to expand my knowledge of something useful." I talked to the counselor and he arranged for me to be interviewed by the teacher who asked me a few general questions that alluded to my character, which I answered quite well, and he asked me why I wanted to take this "select class". I told him I wanted to learn more about operating systems and software that I haven't yet been exposed to. He next asked me what I knew already. I told him I'd programmed in BASIC and C and was familiar with UNIX and MPE XL operating systems. He told me I'd be considered.

As you may have guessed, I was not allowed to enroll in the class. A friend of mine with far less technical knowledge than myself was however. A few days later, my friend talked to the teacher about me and the teacher said, "I got the impression he was some sort of hacker dude; he'll probably just try to crash our networks."

Why do they fear me? Do they fear my knowledge? My political alignment? My attitude? What? Do they dislike males with long hair? Why do they associate hackers with game players?

If I was in their class, I would not have crashed their networks. I would have enjoyed building them. But I am pissed off now. Really pissed off, and you can bet your mother's ass I'm gonna crash 'em now.

Peter The Great

Treat people like criminals and they will act like criminals.

Information Sources

Dear 2600:

Can you tell me a source for the book mentioned in the Winter 1990-91 issue, page 9, *Computer Viruses, A High Tech Disease*?

CH
Los Angeles, CA

Try a Tower Books in your area. They seem to have everything under the sun. Failing that, a decent computer store may be able to help. The book was written by Ralf Burger and published by Abacus. Call some bookstores and libraries with that information and they should be able to guide you to it.

Dear 2600:

We would appreciate being listed among the other publications related to counterespionage, hacking, etc. which we found in your magazine. We stand for free speech and free access to information. *The Eagle* is an independent journal of security investigation and counterespionage published by International Security and Detective Alliance (I.S.D.A.). Our address is PO Box 6303, Corpus Christi, TX 78466-6303.

H. Rochin, PhD, Exec. Dir.

Dear 2600:

On page 11 of the Winter issue, Dr. Williams mentions the Arpanet List of Lists (second column, near the top). That info's old. Here's the official word as of September 1990.

"The file is now available for anonymous FTP from host ftp.nisc.sri.com (192.33.33.53) in directory netinfo. The pathname of the file is netinfo/interest-groups. There is currently no electronic mail access to this file.

"To keep people informed about changes to the file, there is a mailing list for List-of-Lists "update notices". When any updates are made to the file, an announcement message will be sent to the notification list. Copies of the file itself will not be sent to the list. Site representatives who maintain or redistribute copies of this file for their own networks (DDCNet, Xerox, BitNet, MailNet, etc.) and who cannot access the file by Internet FTP may make arrangements to have the file sent to them, if necessary. File copies will normally not be sent to individual users.

"To get on or off the notification list, send requests to:
INTEREST-GROUPS-REQUEST@NISC.SRI.COM.

"To submit new descriptions of mailing lists, to update existing information, or to delete old mailing list information from the List of Lists, send a message to: INTEREST-GROUPS-REQUEST@NISC.SRI.COM.

Flatline

On "Breaking In"

Dear 2600:

After reading your summer 1990 issue, I would like to throw my two cents in. Most of the negative feedback writers compared breaking into a house with "breaking" into a computer. I find this to be an inaccurate comparison.

The reality of the situation is this. The hacker made a phone call. When the computer at the other end answered with a high pitched carrier tone, the hacker's computer made some high pitched whistling sounds back. What are those whistling tones? They are a language, words, a representation of human thought. In America we have an outdated set of laws called The Bill of Rights, perhaps the most radical legal document of all time, but dated, nevertheless. The First Amendment of the Bill of Rights protects a citizen's freedom of speech. A modem and a computer are just as much a tool of language as a typewriter or a printing press, and should be afforded the same protection under the law. If we can agree on that point, let's continue with this stream of logic.

The hacker has called a phone number. The phone is answered and some words are exchanged through the translation of the modems. The computer asks who is this? The hacker replies this is so and so. The computer says how do I know this is so and so. Prove it. Tell me the password we agreed upon when you called before. At this point the hacker must either guess or have access to a password. The hacker repeats a word he has heard that he has gotten from friends, found on another computer, etc. Hearing this word the computer says, okay, you must be so and so. Now ask me whatever you want. The hacker now has use of that computer by false pretenses because he has said the right combination of words. At this point the hacker reads information that is stored on the computer. He decides he wants a copy of a certain document and the computer says okay, since you are so and so, you can have it. The hacker is not stealing it. It is still there on the computer. He has an exact copy made just for him. The hacker is done now. He has what he wants and hangs up the phone.

What has happened? The computer has given the hacker an exact copy of some text the hacker requested over the phone, thinking the caller was someone else. The hacker has lied and said, yes I am so and so, give me a copy of that text. The hacker has misled the computer, but has he broken a law? If so, is the law he has broken legal? That is, does it follow America's fundamental laws laid down in the Bill of Rights?

In my opinion the hacker hasn't broken the law. What the hacker has done is what collection agencies, private detectives, and market research companies do all day long. They call someone up saying they are someone else and if the person who answers the phone is trusting enough to give out information over the phone, then the caller has achieved his goal and received the information he wanted. This may not be very nice, but it is hardly illegal. People who hook up computers to the phone systems should realize that they are hooking their computers into a public system that anyone in the world with a phone can get at. If security is an issue with your information, you should take precautions to protect it. The world is filled with people who act in a way you may consider to be unethical or not nice but they're not breaking the law. Both sides of the issue should recognize that all laws including The Bill of Rights are just words of men and women who want to make you behave in a certain way. Laws are just a way of exhorting power over people who disagree with the law maker. If you disobey their laws you shouldn't be surprised if the power behind the law confronts you. It has come down to a power struggle between the two parties. Behind all laws is the threat of violence and imprisonment. In breaking the rules you run the risk of confronting the beast that hides behind the law.

Computers are amazing devices that are radically shifting the pre-established power structures. Expect a fight for the power.

Scott Alexander
San Francisco, CA

We've been living that fight for more than seven years now. The more people we drag into it, the better. Above all else, we have to fight the knee-jerk reactions that come from people with a very shallow understanding of the technology. We hope more people think the issues through as you did.

Very Concerned

Dear 2600:

I have bought two issues of your magazine and find it interesting and enlightening. I hope to be able to contribute an article someday. I have only your word that you are not, in fact, some FBI/SS/AT&T front to obtain hacker's names and addresses. You *really* should print some information on your operation to provide some assurance to your readers that this is not the case. For instance, are our names and addresses kept in a computer database? Printed files? Could the feds be monitoring what checks pass through your bank account? Do you *have* a bank account? Do you mail 2600 from one central location where packages can be tracked from source to destination? Is there dynamite strapped to your hard drives to be triggered in case of a raid? Inquiring (and paranoid) minds want to know!

Anyway, keep up the good work; it is appreciated nationwide!

Quantum
Austin, TX

We're not running a covert operation here. Everything we do is open to public scrutiny. Our mailing list, though, has never been touched by anyone outside of 2600. Of course, the post office could be writing down every name that ever shows up on a copy of 2600. But that would be pointless and extremely time consuming. If, by some bizarre twist of fate, the government were to actually launch investigations into everyone who received interesting mail, the way to fight such oppression would not be by hiding and allowing it to continue. Challenging authority is our obligation, particularly if that authority is being abused.

Interesting Numbers

Dear 2600:

The ANAC number for the 702 Las Vegas area is 449. Also, the number 662 turns off the phone for a couple of minutes. It is fun to dial 662 at a payphone that is in a busy location and sit back and watch people wonder why it doesn't work. One question: what are COCOT numbers? And do you have any of them for Vegas? How can I find them?

Number 204
Las Vegas, NV

COCOT's are Customer Operated Coin Operated Telephones, in other words, those weird payphones that nobody understands. They frequently answer with some sort of computer when they are called. The computer can do all sorts of things, like tell you how much money it has, allow you to adjust rates, change the time, etc. Some even allow you to listen in on the area surrounding the phone. Most COCOT's don't have phone numbers posted and calls to ANAC numbers are generally disallowed. You might be able to get an operator to tell you the number but the best way is to call somebody collect and have them accept. When they get their bill, the number will be printed out. By the way, another ANAC for Las Vegas is 383-9643.

COCOT Theories

Dear 2600:

When I noticed that George W. from Camden had written to you about a Philadelphia COCOT (somewhere in Center City - I'd love to find it myself), I decided to do some checking of my own. Here are the results of two of the calls I made:

```
CONNECT
T:@*2155465134*81760*CA4107*9522*069*91061570
03733*000003T:@*2155465134*81760*CA4107*9522*
069*9106157000751*000003TN[
NO CARRIER
CONNECT
T:@*2155465134*81950*CA4107*9522*071*91061610
15319*00000:T:@*2155465134*81950*CA4107*9522*
071*9106161015337*00000.TN[
NO CARRIER
```

I believe that the theory your sources cited about the fifth field [069,071] being the number of calls made that day is incorrect. On Friday the 14th, I made several calls to that phone to capture the diagnostic information (on my Tandy 100 - I knew the little critter would always be handy) and the fifth field said 069 the entire day.

However, the second field did change - by increments of 25. I believe that the second field is the value of charges (in cents) that the phone has received. Since a coin box can't hold $819.60, this must either include calling card charges, or the value must be compared by the COCOT service owner to the amount "in" the phone the last time the coin box was emptied.

Finally, to clear up the mystery in the sixth (date) field: the 1 in the middle that you couldn't identify in your reply to George W. indicates the day of the week. I checked this over the course of the weekend and compared George's letter and the New York COCOT reports from your prior issue's letters, and the theory holds.

Antoin Qwerty
Philadelphia

We believe your theories on the second field and the single digit may indeed be correct. But we still believe it's possible the fifth field is counting the number of outgoing calls. There are many payphones, depending on location, that can go through an entire day without a single person using them. It's also possible that the counter, if that's what it is, was malfunctioning.

Valuable Lessons

Dear 2600:

This letter is intended for those people who break the first commandment of the Phone Phreaker's Ten Commandments (*TAP* #86) which is: "Box thou not over thine home telephone wires, for those who doest must surely bring the wrath of the chief special agent down upon thy heads."

Blue boxing is something that is done quite easily here in Ontario and Quebec. All we need to do is dial any phone number (handled by AT&T) that goes to the United States. The two areas in which we can box off of are Springfield, MA (4132T) and Buffalo, NY (7162T). From there you do whatever you want and can with your blue box.

I began blue boxing in 1986 and always boxed from a pay phone. In 1988 I began boxing to Compuserve's CB. Since we only have Tymnet and DataPac which both charge about $10/hour, it was much cheaper to box to a local CIS number at 30 cents an hour. I was even nice to AT&T by boxing to the local number in Springfield, MA so as not to charge them with an LD call. I did all my computer boxing from a local school to be safe, and still obeying the first commandment.

In 1989 I was subscribed to call forwarding. I noticed that when I forwarded my number to an 800 number in the States, an operator would come on the line to a number verification. Hmm, this was interesting. Bell Canada didn't know who I was, so I would give them any number except my own. This made me think that I could get away with boxing at home, because AT&T, if they received my number when dialing over there, would have the number I gave to the operator. I began doing this in November 1989. I began using the blue boxing techniques to call anywhere, anytime. It was a lot of fun.

Now I knew that the Bell equipment here (DMS-100) was recording everything I dialed even as an operator with my blue box. I also knew that Bell should be ringing my doorbell soon. But they never came by. I got rid of my call forwarding, but continued calling from home. Every once in a while I would slow down, because I was making just too many calls.

Well, it finally happened. Recently, a friend of mine called me up and said that Bell Canada Security just visited him. They handed him a nice little bill of $3000. He was dialing 976 services every night for a couple of hours. Then about an hour later Bell Security showed up at my door. I was freaked out and panicking as I went to the door with my parents yelling at me. I looked down at the amount they wanted from me and then almost laughed. They only wanted $350! Boy, what a relief. Of course, they took all my spare change, but at least I was able to pay for it. They only had my calls for the previous month. My theory is that the computer erases the dialing info every month when the bill is made.

I found out that for the whole 418 and 819 area codes, there are only three security people from Bell Canada working them. That's the whole province of Quebec excluding Montreal. I guess that's one reason why it took over a year and a half for them to come visiting, but then again maybe not. I have another friend who just started phreaking this month and was caught for $80. And there were quite a few others being caught that day, the security guy told me. I wanted to ask why it took them so long to come and get me, but of course I wasn't going to let them know how long I was doing this for.

Now if you're asking yourselves why I didn't just say that I didn't have a clue as to what they were talking about, you can blame that on my parents' big mouths who started talking way too much.

Anyway, the point of this little story is that if you are boxing from your home line, you should stop while you're ahead. Hoping that Bell won't come by just isn't enough. If you want to take that risk as I did, then go ahead, but always be prepared to pay the price when security comes by.

The only real bummer in this is that I lost 350 bucks and that I can no longer phreak to bulletin boards. Plus I've gotta start trying to blue box a 2600 over the pay phone, which just isn't as easy as it is at home.

T.15
Quebec

One wonders if there would be as much boxing if access to bulletin boards was made affordable to everyone.

Hacking Water

Dear 2600:

We recently had placed by the local water company, as indeed all users, a new meter that uses a transducer (my guess) at the meter and then a four conductor (looks like Western Electric, gray plastic cover) wire run to the outside of the premise for remote reading.

As a result of some investigating, only three of the four conductors are used of the aforementioned wire. They terminate in a 16 pin, weather protected, black plastic receptacle, marked Neptune ARB.

For educational purposes, can anyone describe how this thing works?

RP
Hiller, PA

Numbers

Dear 2600:

I found an interesting Voice Messaging System at 800-477-4700. It's owned by Pillsbury, Madison, and Sutro. Mailbox numbers are four digits and start with 85. Another number is for those gosh-awful TV evangelists so they can empty out your wallet the 90's way. It's at 800-777-3667. Also, there's a COCOT at (804) 270-4794. Hit 0 to turn on the microphone and hear what's going on.

American Anarchy
Virginia

Another MCI Ripoff

Dear 2600:

MCI is here to save you money. A new service introduced by MCI allows you to have MCI bill you for "regional" calls, i.e. calls within your area code. The benefit is that your volume discount would be combined for the regional and long distance and 800 calls. The reality of the matter is interesting however. For example, a call from Antioch, Illinois to Libertyville, Illinois for 11.8 minutes at 9:23 pm is billed $1.42 by MCI and $.17 by Illinois Bell. The volume discount would reduce the MCI charge by about 14 cents. The MCI way of doing business is a net LOSS of over 650 percent.

Somewhere, MCI's concept of saving money with this program is lost in the reality of their rates.

GR
Libertyville, IL

The Value of 2600

Dear 2600:

One of the great values of your mag is that the back issues I have saved are always full of things I didn't understand a year ago but are invaluable now.

Case in point: your article on UNIX was mostly irrelevant to me in the winter of 1989, but a newly acquired Internet account makes it now altogether essential.

CH
New York

We've always put out the magazine so it doesn't become outdated. While operating systems may change, the basic frameworks will remain intact. And the spirit of hacking links it all together.

Disturbing Observations

Dear 2600:

I found a most distressing feature of many PBX's and similar private networks. When calling to them, they are usually, but not always, identifiable by having extra clicks or different ring sounds than direct CO exchanges.

The problem is that I have *sometimes* noted that I get charged for a completed call before the person actually answers. This becomes even more annoying when getting charged for busy signals (which is how I discovered this problem in the first place). This is also annoying when getting the "number you have reached is not a working number at our complex" message.

This does not always occur, but it seems common enough of a problem to warrant concern, and perhaps, complaints.

My other discovery involves the ANI available to 800 service users. I got a message on my answering machine to call a person at an 800 number. No ID was given for what the company was.

When I called back, I found out it was a credit agency trying to bother me about some past bills (which were improper, but that's another story altogether).

The next day my fax number, which was the line I had called out on, started getting repeated voice phone calls. Seems one of them marked down my ANI'ed number (the fax line), and decided they could use it to harass me.

DB
Flushing, NY

Nobody can call you if you tell them to stop calling you. If they continue, you can report them for harassment. It's as simple as that.

The address to send letters is 2600, PO Box 99, Middle Island, NY 11953. On the networks, mail to 2600@well.sf.ca.us

Last issue one of our readers appealed for bank identification numbers (BINs). We've received several small lists and one huge one for Mastercard. We're told that the Mastercard/Visa list sells for $895. We'll part with the Mastercard half for $5 and if we get the Visa half, we'll offer it all for $10. Meanwhile here's a small sampling.

Here is a list of some BIN's (Bank Identification Numbers) that appear on credit cards. Numbers beginning with 4 are Visa cards, 5's are Mastercards.

4013	BANK OF BALTIMORE
4013	CHEVY CHASE
4019	BANK OF AMERICA
4024	BANK OF AMERICA
4027	ROCKWELL FEDERAL CR UNION
4032	HOUSEHOLD BANK
4060	ASSOCIATES NATIONAL BANK
4070	SECURITY PACIFIC
4071	COLONIAL NATIONAL BANK
4094	AMC FEDERAL CREDIT UNION
4094	COOP SERVICES CREDIT UN
4113	VALLEY NATIONAL BANK
4114	CHEMICAL BANK
4121	ALASKA USA FEDERAL CRE UN
4121	PA STATE EMP CREDIT UNION
4121	PENN STATE EMPLOYEES C U
4121	TANEYTOWN
4122	UNION TRUST
4128	CITIBANK OF SOUTH DAKOTA
4226	CHASE MANHATTAN BANK
4239	CORESTATES
4254	NATIONAL BANK OF NORTHEAS
4254	SECURITY FIRST
4271	CITIBANK
4301	MONOGRAM BANK
4310	BFCU
4311	FIRST NAT BANK LOUISVILLE
4312	BARNETT BANK
4316	LEADER FEDERAL
4316	PIONEER BANK
4316	STANDARD FED
4317	FIRST TIER BANK OMAHA
4327	FIRST ATLANTA
4332	BANK ONE, INDIANAPOLIS
4332	FIRST AMERICAN BANK
4339	PRIMERICA BANK
4342	NCMB-NATIONS BANK
4387	LOCKHEED FEDERAL CRED UN
4387	SANTEL CREDIT UNION
4388	FIRST SIGNATURE BK & TRUS
4388	TEXAS INDEPENDENT BANK
4401	GARY-WHEATON BANK
4413	FIRSTIER BANK LINCOLN
4421	INDIANA NATIONAL BANK
4426	BAR HARBOR BANK
4428	CHOICE
4436	SECURITY BANK AND TRUST
4443	MERRILL LYNCH BANK/TRUST
4447	AMERITRUST
4452	EMPIRE AFFILIATES FED CU
4452	PORTLAND TEACHERS C.U.
4498	REPUBLIC SAVINGS
4502	CIBC
4503	CANADIAN IMPERIAL BANK
4506	BELGIUM A.S.L.K.
4510	ROYAL BANK OF CANADA
4520	TORONTO DOMINION OF CAN
4537	BANK OF NOVA SCOTIA
4538	BANK OF NOVA SCOTIA
4539	BARCLAYS
4544	TSB BANK
4556	CHASE
4556	CITIBANK
4564	BANK OF QUEENSLAND
4673	FIRST CARD
4707	TOMPKINS COUNTY TRUST
4719	ROCKY MOUNTAIN
4721	1ST SECURITY
4726	WELLS FARGO
4784	AT&T
4800	MBNA NORTH AMERICA
4815	MACOM FEDERAL CRED UNION
4820	IBM MID AMERICA FED CR UN
4833	U.S. BANK
4842	SECURITY PACIFIC WASH.
4921	HONG KONG BANK
4921	NATIONAL BANK
5172	FIRST BANK CARD CENTER
5191	BANK OF MONTREAL
5217	CITIZENS FIRST NAT OF NJ
5217	MANUFACTURERS HANOVER
5217	UNION TRUST
5224	MIDLAND BANK
5224	NAT WESTMINSTER BK LONDON
5230	HARRIS TRUST & SAVINGS BK
5232	BADISCHE BEAMTENBANK eG
5239	SOUTHEAST BANK
5242	CHEVY CHASE FSB
5258	NATIONAL BANK OF CANADA
5268	CANADA TRUST
5286	FIRST CARD
5300	BAY BANK
5308	PRIMERICA
5329	MARYLAND BANK OF N.A.
5329	MBNA
5333	BANC OHIO NATIONAL BANK
5351	PROVIDENT NATIONAL BANK
5353	COMMONWEALTH BK AUSTRALIA
5359	CORE STATES
5398	AT&T
5398	AT&T UNIVERSAL
5402	WESTPAC BANKING CORP
5410	CITIBANK
5410	LANGLEY FEDERAL CREDIT UN
5414	STATE STREET BANK & TRUST
5415	UNION BANK
5415	COMERICA
5416	PEOPLE'S BANK
5417	ASSOCIATES NATIONAL BANK
5417	BANK OF NEW YORK
5418	HOUSEHOLD BANK OF CALIF
5418	HOUSEHOLD BANK SALINAS
5420	COLONIAL NATIONAL BANK
5422	HUNTINGTON NATIONAL BANK
5423	UNIVERSITY CREDIT UNION
5424	C B T
5424	CITIBANK
5455	CHASE MANHATTAN BANK

Alien

SECRET FREQUENCIES

by Bernie S.

In the February 8, 1991 issue of "The Leader", an internal newsletter for employees, NYNEX published an article entitled "NYNEX Receives Licenses to Test New Wireless Technologies". In it, Paul Donovan, staff director of NYNEX Science & Technology, was quoted, "Radio technology in the local loop may provide a cost-effective alternative to copper wire" and, "It may also facilitate the provision of new services, adding mobility to our customers."

In a subsequent interview, Donovan conceded that while the FCC (Federal Communications Commission) granted the frequencies for testing specific applications, NYNEX wanted to grab "as many frequencies as possible" to "get (NYNEX engineers') creative juices flowing" so that they "would have plenty of frequencies to work with if we come up with something...."

Despite the appearance of deception (or outright fraud), Donovan justified NYNEX's actions, saying "there's a big market for wireless technologies." Later communication with Donovan and the FCC uncovered specific radio frequencies and locations for testing. *2600* readers in Boston, New York, White Plains, and elsewhere with radio scanners or other VHF, UHF, and microwave receiving (or transmitting!) equipment may want to "tune in" on the telephone company and report on their activities. Mobile and fixed station authorization is granted at power levels up to one watt on the following frequencies. Some Time-Division and Code-Division Multiple Access (TDMA and CDMA) digitally-encoded loop access experiments on 1.858-1.990 GHz are scheduled to begin in mid-1991 and on July 1, 1992. (Read "CDMA: It's Not Just For The Military Anymore", TE&M Magazine, Nov. 15, 1990 for an explanation of these technologies.) The call signs to be used are KF2XBW, KF2XBX, and KF2XEG. Paul Donovan can be reached at the NYNEX Science & Technology Center (914) 644-6165. The FCC can be reached at (717) 334-7059.

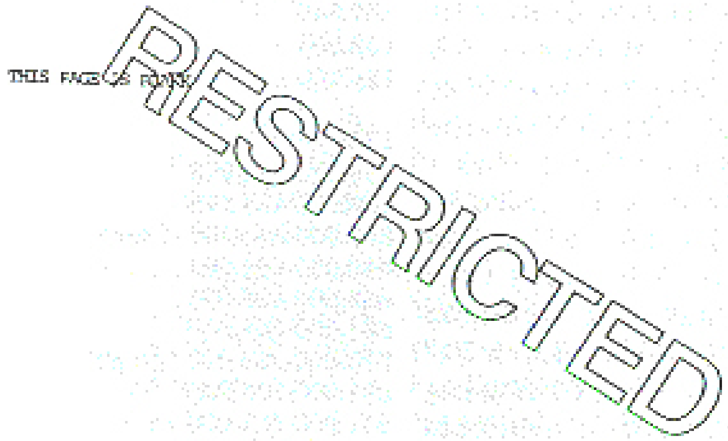
For those interested in just who the FCC has allotted (or sold) the electromagnetic spectrum to lately, a nice 32" x 51" color wall chart covering 3KHz-300Ghz is available for $2.75 from the U.S. Government Printing Office, 710 N. Capital Street NW, Washington DC 20402. Ask for publication number 003-000-00652-2. For other frequencies and information on monitoring techniques and equipment, Monitoring Times (704) 837-9200 and Popular Communications (516) 681-2922 are excellent sources.

NYNEX Science & Technology Experimental Radio Frequencies

VHF (Mhz)
152.510-152.810
152.486
152.834
152.840
157.770-158.070
157.746
158.094
158.100

UHF (Mhz)
454.375-454.975
459.375-459.975
825.000-845.000 (illegal!)
849.000-851.000
862.000-866.000
864.000-868.000
870.000-890.000 (illegal!)
901.000-928.000
931.000-932.000
940.000-941.000

Microwave (GHz)
1.850-1.990 (loop access)
2.110-2.130
2.160-2.180
2.400-2.4835
3.700-4.200
5.725-5.850
5.925-6.425
10.700-11.700
13.200-13.250
17.700-19.700
21.800-23.200
21.200-23.600



THIS PAGE IS BLANK

RESTRICTED

One of the more interesting pages taken from a proprietary phone company document. We intend to shamelessly spread this one around until its value plummets like a rock.

411 - news about phone companies

Regulating Scams

A Senate subcommittee has lost patience with computerized phone calls that try and sell things to people. The Senate Commerce, Science, and Transportation subcommittee heard a whole swarm of complaints from witnesses and senators. Legislation has been proposed by Senator Ernest Hollings (D-SC) to ban computerized sales pitches to residential telephones. Hollings discounted the free speech concerns, saying, "The right is one of privacy for the individual in their home. I don't know of anyone who places a phone in their home in order to receive commercial solicitations." In a bid for a sound bite, Steven Hamm, South Carolina's Director of Consumer Affairs, said, "Computer calls are now the modern form of telephone terrorism." Robert Bulmash, president of the Private Citizen phone consumer group, waxed poetic: "We are nothing more than sources of revenue to an industry that has lost its moral compass. This out of control industry will summon us... by using our conditioned responses to answer the phone as if we were nothing more than Pavlovian dogs with wallets." Wow.

Meanwhile, New York's Public Service Commission is finally taking action against private payphones that don't connect customers to local telephone company operators. A PSC survey showed two thirds of the independent payphones in the state don't pass "0" calls to a local operator but rather to a company operator who often hasn't a clue as to how to handle an emergency call.

And, speaking of scams, according to the New York Daily News, the Port Authority of New York/New Jersey is actually making a commission on fraudulent phone calls. Since they make 18.5 percent on each call from payphones located in the Port Authority Bus Terminal, it's estimated they're clearing more than $2 million in profits from these calls. That's more than they get in rent from retail stores in the structure.

The FCC is finally introducing a proposal that providers of 900 service introduce each call with an explanation of the cost involved. If the customer hangs up at that point, he will not be charged. A final decision is expected by the end of the year. Owners of 900 numbers have come out against the plan, saying that people would hang up without good reason. Go figure that one out when you find time. Meanwhile, we'd like to propose a compromise. Since more switching systems are becoming integrated and filled with intelligence, it should be possible to begin relaying pricing information while the actual call is being routed. In other words, your central office would see a call to a particular 900 number being placed, would consult a pricing table, and, while the call is being routed through the long distance lines, would play a recording to the caller. Of course, it's only a matter of time before some clown proposes sticking an advertisement there for all other calls. Perhaps we shouldn't say any more.

AT&T Wants The World

AT&T wants to get permission from the U.S. government to start providing phone service to Vietnam, one of three countries that cannot be called from the United States (the others are Cambodia and North Korea). AT&T says that unlicensed operators are providing service through Canada, Japan, France, South Korea, Hong Kong, and Australia and they're making lots of money in the process. We can imagine AT&T's frustration being forced to stand on the sidelines.

Advances in the U.K.

British Telecom has instituted what it calls a "fairer" system of paying for calls to directory assistance. Customers who use the service will be charged 37.8 pence plus 15 percent tax for up to two numbers. Now, after reading that, you would think that you would get charged that rate for two requests. Not so. Whenever you use directory assistance, you can ask for up to two numbers. Most people, however, use the service to get a particular number they need at the moment. So, despite BT's clever way of phrasing it, it's likely the service will cost 37.8 pence *per request*. It is a rather inventive way of making less seem like more. Phone companies in the States will no doubt take note. By the way, calls to directory assistance from pay phones and from blind or disabled people will still be free. And rates for various other calls will be reduced slightly to make up for the new charges. BT has introduced a couple of services for those people who use directory assistance heavily. Phone Base gives them direct access to the company's computerized system and Phone Disc is an electronic version of the phone books on CD ROM.

One apparently positive move that BT has made recently is to eliminate the surcharge on their calling cards, known as BT Chargecards. Cardholders can just dial 144 and follow voice prompts to enter their account number, PIN code, and phone number they want to reach. They will be charged the same rates as a regular payphone call, which we hope is fairly close to residential rates. If not, then this is just more deception.

Last year, British Telecom's trunk network became "the first telephone system in any major industrialized country to become fully digital." Now they've hit the halfway point in switching their local exchanges from electromechanical to digital. Yet only 75 percent of BT's customers have the capability of getting itemized bills.

And just as in the United States, people in England are having problems with "premium" services that bill huge amounts of money to unsuspecting customers. The special area codes for these services are 0898, 08364, 0839, 0881, 0066, and 0077. (0800 calls are toll free.) In the areas that have been digitized, it is now possible to block access to these numbers. Still more proof of evolution. By the way, the cost of pressing the right computer keys to accomplish the blocking will be underwritten by raising the rates of the blocked numbers!

New Services

Sprint has a new service called 900 to 800 Transfer that allows callers dialing a 900 number to be transferred to a toll-free 800 number. Why would anyone want to do this? The thought is that callers will dial a 900 number to get information about a particular item and then be transferred to an 800 number when they agree to buy it. The caller only gets charged for the time spent on the 900 number, at least in theory. The only way to really find out is to keep a pen, pad, and clock by the phone at all times.

Another new service Sprint is offering is for the benefit of hotels. It's called Answer Detect and it does what AT&T and the regional Bells have been doing for years: bill the call from the moment the called party picks up. Many hotels currently use the equivalent of a pen register tied into a computer. If you stay on for a certain amount of time, it's assumed that the call was answered and you get billed. Accuracy tends to go out the window in hotels because of the need to bill quickly. The new Sprint service will work in conjunction with the hotel's existing phone system.

New York will be the first city in the United States to test out prepaid charge cards on its payphones. Just as in Europe and Asia, charge cards (called NYNEX Change Cards) will be available for sale at newsstands and other stores. Each phone will have a little screen that displays the amount remaining on the card and as each call progresses, that amount will go down. The test is scheduled to begin in September with 60 to 80 phones. We hope they avoid the mistakes made in countries like France, where it is impossible to use any payphone without a card. If cards, for whatever reason, are unavailable, there are no alternatives. We would hate to see such an oppressive system forced down our throats.

Another technological advance is being ushered in by Illinois Bell. Customers are now able to pay their bills over the same phone line they're paying for! By calling an 800 number and entering their secret ID, they can transfer money directly from their checking accounts to the phone company. Would you trust the phone company not to ever take matters into their own hands since they obviously have all the information they need to get at your money?

The new AT&T calling cards are out. "In order to comply with government requirements, AT&T is no longer sharing card numbers with your local telephone company," the mailing reads. As a result we now have 14 digit numbers that bear no resemblance to telephone numbers. But, contrary to what they say, these new numbers are accepted by New York Telephone, which at last report was a local telephone company. For a "demonstration" of your calling card, you can call 800-255-3439. All cards seem to begin with 836 or 838. The next digit is either a one or a zero. The next six digits can be any number. The last four comprise the PIN. They, too, can be any number. Each card also has an international number which begins with 891253 followed by the card number without the four digit PIN. One number follows this which is a check digit. Then there is a two digit authorization code at the end. There are two other formats for the AT&T calling cards. One has 21 digits and always begins with either 891288 or 891253. This is followed by ten digits, a check digit, and a four digit PIN. Then there is a 17 digit version that begins with either 288 or 253, followed by ten digits, then a four digit PIN.

Southwestern Bell will be testing out a service called Message Express from its payphones. Customers will be able to leave a message when they encounter a busy signal. It won't be automatic, though. Callers will have to dial an 800 number that will be posted on the phones and leave a one minute message. Payment will be by credit card only. COCOTs have been offering similar services for quite some time. We presume Southwestern Bell will have an advantage since they can instantly detect when a phone is no longer busy, while COCOT companies have to keep trying to get through periodically.

Corporate Litigation

In one of the silliest cases we've heard of in a while, Mitsubishi is trying to sue AT&T because of security problems on an AT&T System 85 PBX. More than 30,000 unauthorized calls to places like Pakistan and Egypt were made at a cost of more than $400,000. Mitsubishi is claiming that AT&T never told them something like this could happen. According to one of Mitsubishi's lawyers, they were completely unaware that their system was vulnerable to attack. We believe they should be branded with that as part of a slogan: "Mitsubishi: We're Completely Unaware." If AT&T had refused to help them or if their equipment was impossible to safeguard, we could see Mitsubishi's point. But here it seems like they're just trying to pass the buck and get out of paying a huge bill for their ignorance. While we're on the subject of ignorance, or should we say maliciousness, both *New York Newsday* and New York State Police investigator Donald Delaney have repeatedly blamed such activity on phone phreaks. In fact, *Newsday* goes so far as to define phone phreaks as people who often make their living from figuring out how to make free calls. We don't expect people who are so completely out of it to understand what a phone phreak is. But we cannot tolerate having blatant lies spread for the purposes of selling papers or getting warrants more easily.

The Times of London is no better. They define hackers as "people who steal computer passwords to break into international databases and use services illegally." According to them, George Snow received a phone bill for 8,000 pounds because somebody guessed his password on British Telecom's Dial Plus service which allows callers access to international computer services via a local call. His password, incidentally, was Superman. Dial Plus customers have to sign an agreement saying they will not use easily guessable passwords. But Mr. Snow had signed up for the system prior to that and in addition, BT had approved the password themselves. We see the phone company as being responsible for the charges incurred, primarily because this is a consumer-based service. Different rules have to apply in these kinds of situations. You cannot penalize someone a huge amount of money because they chose a stupid password. However, a company that is in the phone or computer business has the obligation to see to it that its users are utilizing adequate security. If they fail to do this, as Mitsubishi apparently did in the case above, then the penalty is theirs.

In another pair of lawsuits that shows how out of control the telephone industry has gotten, AT&T is suing a COCOT company for not paying more than one million dollars of fraudulent charges. The company, North American Industries of Great Neck, New York has turned around and sued New York Telephone for not giving COCOT companies a fair deal. In an interview on WBAI's *Off The Hook*, North American Industries president Barry Berman said that fraud is an especially big problem for independent pay phones. The installation isn't very secure in most cases. All a person has to do is clip into the connection before it reaches the payphone and they can make all the calls they want. Since the payphone technology is completely within the COCOT, anyone getting access to the line before it reaches the COCOT wouldn't run into any restrictions. By contrast, New York Telephone payphones are controlled from the central office. No matter where someone taps into it, the phone company knows it's a payphone and won't allow calls to be placed without the proper coins or beeps. It may be a wild guess on our part but perhaps when independent pay phones and alternate long distance companies are given the same access to technology that the regional Bell companies and AT&T have, they may stop ripping people off so much. Right now, it seems to be the only way they can stay in business.

A great example of this is currently making the rounds. It seems that AT&T has a three-digit calling card: 15x (x being any number) followed by a # key will allow any zero plus call to go through from home phones. (We're told all it does is bill back to the originating number.) This does not work from regional Bell pay phones but it does work from a lot of COCOTs. Which means that again the COCOT owners are getting stuck, this time directly by AT&T.

COCOT and PBX Features

We thought you might be interested in some of the features being advertised in COCOT literature. Selling points include: being able to accept nickels, dimes, and quarters (wow!); voice synthesized instructions; optional coin free access to the operator, emergency services, and 800 numbers (we can't understand why any payphone operator would want, let alone be allowed, to make essential services optional - this "feature" should be illegal); being able to detect busy signals, answer supervision, ringing, and intercept recordings; storing preset speed dial numbers; and, of course, remote programming capabilities.

The CFCA (Communications Fraud Control Association) is passing around some safety tips for corporate PBX's: Assign authorization codes randomly on a need-to-have basis and limit the number of calls using these codes; Never match codes with company telephone, station, or badge numbers; Instruct employees to safeguard their authorization codes, which should be assigned individually, not printed in billing records; Codes should be frequently changed and cancelled when an employee leaves the company; Remote access trunks should be limited to domestic calling and shut down when not in use; Use the time-of-day PBX option; Use a system-wide barrier code, followed by an authorization code with the most digits your PBX can handle; Use a non-published number for remote access lines; Use a delayed electronic call response, which is the same as letting your phone ring four or five times before answering; Try hacking your own system to find weaknesses, then correct them.

Story of the Year

Earlier in the summer, the owners of the Long Island Pet Cemetery in Middle Island, New York were indicted for allegedly not burying pets like they said they were doing. Instead of putting Spot or Fido in the ground by his/her tombstone or giving the ashes to the bereaved owners, they were said to have dumped up to 250,000 carcasses in a mass grave and given random mixed ashes to the pet owners. Needless to say, this has not gone over well. (The Long Island Pet Cemetery is right next door to 2600's post office boxes and there have been vigils, demonstrations, and near-riots there over the past couple of months.) But in addition to this, the cemetery owners are accused of gaining remote access to their competitor's answering machines late at night in order to get the names and numbers of dead pet owners before their competitors did. It's a nasty business.

Another Great 900 Number

Our favorite press release of the week begins: "Have you ever arrived at the hotel at which you told everyone you would be staying, only to find that a mistake had been made requiring you to stay elsewhere? Has your daughter been on a camping trip at the same time you were required to leave the country, and you needed to tell her something personal first? Or, did you ever want to contact an old friend only to discover that they had moved? A new service called 900 JOT DOWN will aid all the above problems as well as greatly expand an individual's ability to send and receive secure messages." The calls cost $1.95 for the first minute and 95 cents for each additional minute. You would have to be a Class A Fool to use this service as every aspect of it can be easily accomplished for significantly less. When you call in, you can press 1 to receive an identification number and password for their system. (That's the only feature we can't accomplish for less!) Pressing 2 allows you to "receive another subscriber's repository of phone numbers". This means for $1.95 you can find out somebody's phone number(s). (In the example of trying to track down an old friend who had moved that was given above, the company neglects to mention that the old friend has to be subscribing to the same service! How many old friends do you suppose you've lost touch with who are subscribing to the same brand new service as you?) By pressing 3, you can leave a voice message for a subscriber. They make it clear that anyone can spend $1.95 to leave a brief message, not just subscribers. Just like calling an answering machine, except you get to spend so much more. Plus you have to enter the subscriber's identification code after pressing 3. We hope you have a touch tone phone. Pressing 4, entering your identification code, and entering your password allows you to retrieve your messages. Any decent answering machine will allow you to do the same thing at no cost other than the phone call. Various voice mail services allow you almost unlimited access for charges of around $15 a month. Many of these have additional services, such as paging features. If you were to call this 900 service only eight times within a month, either to leave messages or retrieve them, you would be spending more. By pressing 5, you can "update your personal phone or repository" which we presume to mean update your phone numbers so other subscribers can find out what they are. One of the marvels of the communications age is the ability to convey information for free. Believe it or not, it does not cost $2.00 plus to get somebody's phone numbers or to announce them to the public. There are too many preferable methods to mention here. The final selection can be accessed by pressing 6, which gives you "a secure, private phone line for outbound calls". Unless they've somehow managed to get access to secure phone lines used by the military, most consumers won't have to look far to find phone lines that cost less than 95 cents a minute ($1.95 for the first). And, should anyone believe their calls are somehow more secure because they're being made through a third party, read our recent Winter and Spring issues that detail why this is not so (concerning the 900 STOPPER "service"). If you believe this kind of thing is worthwhile, you'd probably be interested in the computer version, reachable at 900 JOT PORT.

Japanese Numbers

Some "home country direct" numbers from Japan: United States: 0039-111; Hawaii only: 0039-181; Canada: 0039-161; United Kingdom: 0039-441; France: 0039-331; Italy: 0039-391; Netherlands: 0039-311; South Korea: 0039-821; Hong Kong: 0039-852; Taiwan: 0039-886; Thailand: 0039-661; Singapore: 0039-651; Australia: 0039-611; and New Zealand: 0039-641. To make regular international calls from Japan, dial 001 plus country code, city code, and subscriber number.

Customs of the U.S.A.

According to the *San Antonio Light*, if you live in San Antonio and want to report someone who owns "gangster-type weapons such as machine guns and sawed-off shotguns", you can call 666-GUNS. The Gun Owners, a Springfield, Virginia based publication took exception to the phone number. "Does the BATF [Bureau of Alcohol, Tobacco, and Firearms] have a fascination with that number? A few years ago, the BATF had also made a sample badge for an emblem - the number on the badge was 666. Now they are using that same number again, presumably as a way to intimidate people."

To shed light on another issue, we've heard many stupid ideas in this so called War Against Drugs. Some cities have made it impossible for payphones to receive calls. That way, drug dealers won't be able to receive calls and there will be less drugs. Other cities have eliminated touch tone payphones and replaced them with old fashioned rotary phones. That way, drug dealers won't be able to use touch tones to activate other drug dealers' beepers. This will result in less drugs. Certain officials have suggested outlawing beepers for anyone under 18. Less beepers means less drugs. If, by some miracle, drug dealers manage to survive in a rotary dial, non-callback, beeperless environment, the latest brainstorm will stop them dead. Illinois Bell figures that anybody putting money into a phone at night must be a drug dealer. Therefore, they are beginning a new policy in Chicago's poorer neighborhoods: no coins will be accepted between 7:30 pm and 4:00 am. The hours were originally 6:00 pm to 6:00 am. According to the *Chicago Sun Times*, there has been no opposition to this idea. As one businessman put it, "I think it's a great idea. Anything to cut down on drugs." Anything.

The Outages

We never got as many phone calls as we did this summer concerning the recent phone outages that affected various areas of the country. Everybody wanted to know if hackers were responsible. And, even if they weren't, could they be in the future? We told them we couldn't make any promises but it is pretty certain that such outages and foulups will be commonplace in the years to come. Most of it will be due to the usual stupidity and short-sightedness on the part of those who implement these systems. As anyone who has ever installed a new operating system on a personal computer can tell you, there are always transitional problems to contend with. Without exception. For major phone companies not to have an easy way of getting around the problems that occurred when a new switching system (Signalling System 7) was implemented is nothing short of criminal. After all, telephones are life lines for nearly everyone. Yet those in charge are content to look at the whole operation as another big computer system. According to Richard Firestone, chief of the Federal Communications Commission's Common Carrier Bureau, the recent failures are actually a sign of progress because they were caused by upgrades. Doublespeak City.

Firestone said the prospect of an independent backup system was out of the question because of the expense involved. This FCC spokesman also suggested that those who needed absolute -reliability should go out and buy their own backup system. About the only positive thing this guy did was stop short of imposing fines on people who complain.

For the record, the problems were related. There was a flaw in software obtained from DSC Communications of Plano, Texas. It was never tested adequately by anyone. California, Virginia, West Virginia, Maryland, Pennsylvania, North Carolina, and Washington DC were all affected at some point by the flaw.

Another Outage

This advertisement was placed in various St. Louis papers on June 9, 1991:

AN OPEN LETTER TO OUR BUSINESS CUSTOMERS:

At Southwestern Bell Telephone, we've built a high standard of customer service and we take pride in that. Unfortunately, we recently experienced a rare failure in a computer system that transmits data.

As a result, about 750 St. Louis-area business customers lost access to important day-to-day services. For those of you whose service was impaired, that failure translates to a disruption in your operations and, at best, an inconvenience to your customers. We apologize for letting you down in this instance. Though the problem lingered longer than any of us would have liked, we made every effort to see that it was fixed as quickly as *possible. Our technicians worked around the clock, logging more than 2,500 hours, to correct the problem. We enlisted the help of experts from across the country.*

Still, I know that even though we pulled out all stops to restore service, you would rather it not have happened at all. So would we. Now that service has been restored, our focus has shifted to further upgrading the system's reliability. While some of the solutions may take time to complete, we will persist until the service we provide meets your high standards and ours. In the next few days, we will individually contact customers whose service was interrupted. We want to share with you our plans for improving the system, and we want to hear your comments on how we can continually improve our service to you. We are committed to earning your confidence once again.

Sincerely,
Randy Barroy
President
Missouri Division
Southwestern Bell Telephone

Among the casualties of *this* screwup was Arlington Park Racetrack near Chicago. They had to turn away their customers because the phone problems crippled its computerized betting operations. Customers were not very happy. And, according to experts, Southwestern Bell is not liable unless it can be proven that they did this deliberately. In addition, ATM's were shut down, the entire Federal Reserve System was slowed down, and banks were cut off from their main computers. While Randy Barroy was more than happy to tell everyone how many hours Southwestern Bell's technicians logged, he neglected to mention just how long their computers were down for. Six days.

A Southwestern Bell spokesperson said, "We don't anticipate this happening again." They sure didn't anticipate it the first time.

But at least we know they're in touch with their customers. "You would rather it not have happened at all." Such a keen sense of perception does not come cheap.

Caller ID Pushers

A recent letter to the Public Service Commission from New York Telephone argued for the implementation of Caller ID and CLASS services as soon as possible. "The current balance of privacy between calling and called parties is the result of technology, not social policy. In early telephone service, all calls were placed through operators, who identified the caller to the called person. Party line service, which three quarters of American telephone customers had in 1950, provided a check on the anonymity of the caller, since outgoing calls could not be depended upon to be private. By the 1960's, telephone technology tipped the balance in favor of the caller when direct-dial, single party telephone service became widespread, as did annoyance calls. Technological change, which caused the imbalance, now can help improve it, in the form of Caller ID."

They then use this as justification for not implementing all-call blocking for customers who want it. All-call blocking would mean that all calls made from a particular number (except to 911) would not transmit the phone number to the called party. New York Telephone wants to instead offer per-call blocking, meaning that the caller would have to dial a special code (*67) before every call they wanted to make without transmitting their number. By doing it this way, New York Telephone reasons, less people would block their numbers and the called party would know that the caller had made a conscious effort to block theirs.

Why are the phone companies suddenly so concerned about all of these harassing calls that everyone is allegedly getting? We think they're much more concerned about selling their product to the public. If too many people elect to block their phone numbers, their product won't really be that appealing. But if it's made more difficult to block your number and if those who do are made to feel as if they're guilty of some crime, more people will subscribe and the phone companies will rake it in.

If you still believe that this is about privacy, consider the two bits of misinformation all of the phone companies insist on spreading. 1) People who block all of their calls won't be able to transmit their number in an emergency. Not true. Enhanced 911 passes your number to the police regardless of whether you use call blocking. This service is becoming available throughout the country. Caller ID is irrelevant in these cases unless callers are calling non emergency numbers. And that wouldn't make much sense in an emergency, would it? 2) This will spell the end of harassing phone calls. Totally untrue. All a caller has to do is call from a payphone, a calling card, a long distance company, or simply be out of the immediate area!

Since those people who are up to something or who want to remain anonymous will always manage to do so, the phone companies would be better advised to promote the service as something positive for those people who want to announce their arrival before they begin speaking. And as for what society wants or needs, let's leave that up to society, not the phone company.

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center—from 5 to 8 pm in the lobby near the payphones. 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162, 212-308-8184. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

SPY SHOP CATALOGUE: Packed with equipment, items, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, stun guns, room monitors, decoding devices, analyzers, covert tracking systems, defense sprays, caller ID, people tracers - find anyone anywhere! Detection systems, tap trap, voice changers, scramblers, secure phones, and much more. Send $5 check or money order to: Bug Busters, PO Box 978, Dept. 2-6, Shoreham, NY 11786. FAX 516-929-0772.

WILL PAY $10,000 for "mind radio" computer program and schematics. Call Mike at 212-533-4351.

KNOW WHO'S CALLING! The Call Identifier has the answer. Displays caller's phone number when your phone rings. Stores phone numbers with date and time of call. $79.95. $10 for 2600 subscribers. E.D.E., PO Box 337, Buffalo, NY 14226. (716) 691-3476. Surveillance-Countersurveillance equipment catalog $5.

CAN SUPPLY software and computer hardware of any kind below wholesale prices. I am looking for sales people. If you can find me buyers, I will work out a percentage. Would like to correspond with hackers in Switzerland, Germany, Japan, and France. Anybody with access to stealth bomber technology or access to Los Alamos National Laboratory in New Mexico and/or Lawrence Livermore Labs in San Francisco. K. Henderson, PO Box 265, Agoura Hills, CA 91301. 818-889-8361.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. The first book on how to write them! 190 pgs, soft cover, with full IBM PC source code. $14.95 postpaid, or ask your local bookstore to order it. (ISBN 0-929408-02-0) American Eagle Publications, Box 41401, Tucson, AZ 85717.

TECHNICAL SURVEILLANCE COUNTERMEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800-US-DEBUG.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

TAP BACK ISSUES, complete set Iss 1-91, high quality, $50. SASE for index, info on other holdings. Robert H., 1209 N 70th, Wauwatosa, WI 53213.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

OLD TAPES of telephone recordings, rings, busys, etc. wanted for radio programs. Also, current recordings and funny phone calls welcome. Send to Emmanuel, PO Box 99, Middle Island, NY 11953.

SEE ME HERE.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 10/15/91.

when hackers ride horses: a review of *cyberpunk*

Cyberpunk: Outlaws and Hackers
on the Computer Frontier
by Katie Hafner and John Markoff
$22.95, Simon and Schuster, 354 pages
Review by The Devil's Advocate

The exploits of Kevin Mitnick, Pengo, and Robert Morris have become legendary both in and out of the hacker mainstream. Until now, however, hackers have had to worship their idols from afar. *Cyberpunk: Outlaws and Hackers on the Computer Frontier* unites hackers in this true-life testimony by presenting an in-depth up-front view of these "techno-menaces" without the overreactive doomsday prophecies that usually accompany such a work.

Cyberpunk is a fitting sequel to Steven Levy's classic *Hackers*. Whereas Levy's treatise addressed the origins of hacking in its infancy, *Cyberpunk* is the New Testament depicting hacking as it is in the here and now. More than just a synthesis of current trends, however, *Cyberpunk* depicts the hacking lifestyle and cyberpunk culture that has evolved alongside our boundless fascination with computers and information. *Cyberpunk* portrays hackers as they really are: *real* people with lives not unlike our own. Yes, hackers have emotions, desires, and problems just like we do. No, they're not all computerholics or socially inferior psycho cases withdrawing into the depths of the "matrix" to escape from reality. If anything, *Cyberpunk* will blast away some of the antiquated stereotypes that have persisted throughout the '80s.

In *Cyberpunk*, all the central characters identify closely with their science fiction counterparts. Indeed, the (Inter) "net" is one of the many threads that tie the lives of Mitnick, Pengo, and rtm (Robert Morris) together. The most interesting story by far is that of Pengo, a West Berliner who, more than any other character, epitomizes what it means to be a cyberpunk. Pengo was truly a computer outlaw: aspiring to the likeness of the character Case in William Gibson's *Neuromancer*, traveling the net in search of data to sell, and owing no allegiance to country or nation. Readers familiar with *The Cuckoo's Egg* will find this section particularly interesting. *Cyberpunk's* account of the West Berlin hackers makes *The Cuckoo's Egg* look like a fledgling fluttering in the quirkiness of Stoll's campy prose. Now readers can see what it was that Stoll himself was trying to vicariously experience through his own terminal. *Cyberpunk* provides the missing pieces and puts Stoll's *Cuckoo* into perspective.

The book confirms what hackers on all coasts have known and preached for years: that a computer system's worst enemy is its users. Nearly every system was hacked by exploiting poorly chosen passwords or bugs in the operating systems. Interestingly, *Cyberpunk* also confirms that the authorities amount to only so many bumbling Keystone computer cops desperately trying to match wits with misfits. The fact is that everyone described here got busted because they either talked too much or were betrayed by close friends. Without such help, the long arm of the law appears to be nothing more than a wet noodle.

Perhaps the central weakness of *Cyberpunk* is its somewhat blatant bias and lack of objectivity. Time and time again, readers will encounter the authors' own prejudices slipping through the cracks between the lines. Although no one is innocent in *Cyberpunk*, readers will easily get the impression that Mitnick is the sinner of the three. This is despite the fact that Mitnick's exploits appear equal, if not less damaging, than those of the others. Unfortunately, the bias rears its ugly head in a number of passages, a telltale sign that the authors appear to be more incensed with Mitnick's attitude than with anything else. It is also no coincidence that Mitnick is the only central character that refused to be interviewed for the book.

Despite this weakness, *Cyberpunk* remains a thought provoking looking glass into the lives of the most interesting people in the Information Age. The true tales of these harbinger hackers will leave readers spellbound while they eagerly await a sequel.

PURE CYBERFICTION, SAYS MITNICK

The following are comments by Kevin Mitnick on the portions of the book that are about him.

I am sad to report that part one of the book *Cyberpunk*, specifically the chapters on "Kevin: The Dark Side Hacker", is 20 percent fabricated and libelous. It seems that the authors acted with malice to cause me harm after my refusal to cooperate. Interestingly enough, I did offer to participate as a factual information source if I was compensated for my time, but the authors refused, claiming it would taint my objectivity. So consequently, I declined to cooperate.

However, my co-defendant, Lenny Dicicco, of Data Processing Design, chose to participate probably in the hopes of being recognized as a "hero" who was responsible for bringing me to justice. Lenny seemed to have gained unquestionable credibility when he turned us both into Digital and the U.S. government. Surprisingly, he who "snitches" first is believed to be totally credible by the U.S. government. Case in point: most of the U.S. government's argument to hold me without bail was based on false information (this was later admitted by the U.S. government). This information, I believe, was mainly from Lenny Dicicco and his cronies (Steven Rhoades of Pasadena, CA). So once Lenny lied to the U.S. government he couldn't change his story, since he could risk violating his plea agreement or being indicted on federal perjury charges. Unfortunately, this probably resulted in a lot of false material being introduced by Lenny Dicicco, and Katie Hafner printing it as factual information in *Cyberpunk*.

Katie probably wasn't happy with me for refusing to help her, so part one of the book was written with a strong anti-Mitnick, pro-Dicicco bias. This bias rewarded Lenny for his participation but robbed the readers of the real truthful facts! Lenny was described simply as an "errand boy" in our hacking exploits. This is the furthest thing from the truth! Lenny was just as culpable as me; we were hacking partners for over 10 years. What do you believe?

Let's examine some interesting cover-ups Katie Hafner did for Lenny Dicicco:

1) In the galley copy of *Cyberpunk*, Katie Hafner wrote that Lenny Dicicco was going to work for DEC as a computer security consultant in lieu of court ordered restitution ($12,000). Why was the information eliminated from the final printed copy? Probably DEC wouldn't be happy with Lenny - he did provide Katie with enormous detail regarding the DEC break-in. Not to mention the controversial issue regarding DEC hiring the person that penetrated their network.

2) On page 80, Katie wrote that Lenny Dicicco obtained a false identity to obtain a job that required a "clean" driving record. The name Katie printed was "Robert Andrew Bollinger". This is false! The name of the "false" identity was "Russell Anthony Brooking". But why would Katie print this erroneous information? I know why! Lenny was working under the fraudulent identity (Russell Anthony Brooking) while he was collecting unemployment under his real name (Leonard Mitchell Dicicco) thereby defrauding the State of California! Now Katie wouldn't want the "truth" to be known - it might cause Lenny to refuse to participate in possible upcoming interviews and talk shows promoting her book.

I could go on and on, even simple verifiable information. For example, on page 84, Katie describes a scenario where I asked Bonnie out on a date. To paint an unsavory picture, she stated that I was always eating in the computer room when talking with Bonnie. Very interesting, since at the Computer Learning Center of Los Angeles, no food or drinks can *ever* be brought into the computer room. Even though this scenario is pretty insignificant, it demonstrates the introduction of inaccurate and misrepresented facts.

Again, when describing my arrest at USC in 1982, Katie wrote on page 71 that I taunted Mark Brown (USC System Manager) in his investigative techniques. This is truly amazing, since I never spoke with Mark Brown.

There are many, many false statements, misrepresentations, and inaccurate stories in part one of this book. I could only say it is sad that the authors were too cheap to compensate me for my time. Instead they hid under the ruse of "tainted objectivity". This resulted in my refusal to participate.

In summary, *Cyberpunk* is an interesting read-through as long as readers understand this purported non-fiction book is not what it claims to be. Part one of the book is 20 percent inaccurate. I believe the authors acted with malice due to my refusal to participate for free. Katie Hafner's only hope was seeking the cooperation of my convicted co-defendant, Lenny Dicicco. She did gain his full cooperation which resulted in a strong bias and misrepresentation of facts.

OUTDIALS

by Net Runner

PC-Pursuit and Datapac outdials make up the bulk of easily accessible outdials from Tymnet. The Datapac outdials are often shaky but the PC-Pursuit ones tend to be stable.

On occasion, if you enter an additional .01 at the end of a PC-Pursuit NUA, you may get global outdialing, allowing access to anywhere in the U.S.A.

Upon connecting to a PC-Pursuit or Datapac outdial, you should change to 8N1 bits. This makes life easier on BBS's.

PC-Pursuit outdials have a menu system. Hit % after connecting. It will respond with: "HELLO: I'M READY" followed by a star. At the star, enter a D for dial or R for redial.

PC-Pursuit Outdials

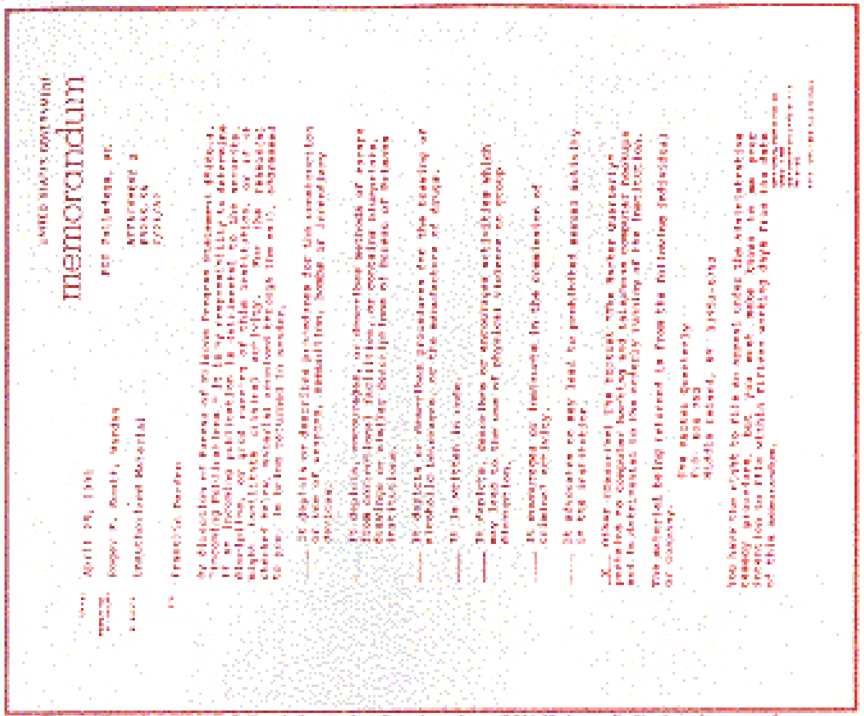
(3110 is Telenet identifier, NPA follows. Baud rates vary.)

311020100001
311020100301
311020100022
311020200115
311020200116
311020200117
311020300105
311020300120
311020300121
311020600205
311020600206
311020600208
311021200315
311021200316
311021200028
311021200412
311021300412
311021300413
311021300023
311021400117
311021400118
311021400022
311021500112
311021500005
311021500022
311021600020
311021600021
311021600120
311030100020
311030300114
311030300115
311030300021
311030300022
311030500120
311030500121
311030500112
311031200410
311031200411
311031200024
311031300214
311031300216
311031300024
311031400005
311031400421
311031400020
311040400113
311040400114
311040400022
311040800111
311040800021
311040800110
311041400020
311041400021
311041400120
311041500005
311041500216
311041500011
311041500106
311041500224
311041500108
311041500215
311041500117
311041500217
311041500220
311041500023
311050300020
311050300021
311050300120
311060200020
311060200021
311060200022
311060200023
311060200026
311061200120
311061200121
311061200022
311061700311
311061700313
311061700026
311071300113
311071300114
311071300024
311071400023
311071400004
311071400024
311071400119
311071400213
311071400124
311071400120
311071400102
311071400210
311071400121
311080100020
311080100021
311080100012
311081300020
311081300021
311081300124
311081600104
311081600221
311081600113
311081800020
311081800021
311091600007
311091600011
311091600012
311091900020
311091900021
311091900124

Datapac Outdials

(3020 is Datapac identifier, NPA is in parentheses. Baud rates vary.)

302069200902 (204)
302069200901 (204)
302072100900 (306)
302072100901 (306)
302071100900 (306)
302071100901 (306)
302063300900 (403)
302066300901 (403)
302058700900 (403)
302058700901 (403)
302091600901 (416)
302091600902 (416)
302038500900 (416)
302038500901 (416)
302074600900 (506)
302074600901 (506)
302082700902 (514)
302082700903 (514)
302035800900 (519)
302035800901 (519)
302029500900 (519)
302029500901 (519)
302033400900 (519)
302033400901 (519)
302067100900 (604)
302067100901 (604)
302085700901 (613)
302085700902 (613)
302038500900 (613)
302038500901 (613)
302078100900 (709)
302078100901 (709)
302076101900 (902)
302076101901 (902)
302038500900 (416)
302038500901 (416)



UNITED STATES GOVERNMENT

memorandum

FCP Talladega, AL

Attachment 2
P5266.05
7/31/85

DATE: April 28, 1991

REPLY TO ATTN OF: Roger P. Scott, Warden

SUBJECT: Unauthorized Material

TO: Franklin Darden

By direction of Bureau of Prisons Program Statement 5266.4, "Incoming Publications," it is my responsibility to determine if an incoming publication is detrimental to the security, discipline, or good order of this institution, or if it might facilitate criminal activity. For the reason(s) checked below, material received through the mail, addressed to you, is being returned to sender.

___ It depicts or describes procedures for the construction or use of weapons, ammunition, bombs or incendiary devices.

___ It depicts, encourages, or describes methods of escape from correctional facilities, or contains blueprints, drawings or similar descriptions of Bureau of Prisons institutions.

___ It depicts or describes procedures for the brewing of alcoholic beverages, or the manufacture of drugs.

___ It is written in code.

___ It depicts, describes or encourages activities which may lead to the use of physical violence or group disruption.

___ It encourages or instructs in the commission of criminal activity.

___ It advocates or may lead to prohibited sexual activity in the institution.

_X_ Other (Describe) The booklet "The Hacker Quarterly" pertains to computer hacking and telephone computer hookups and is detrimental to the orderly running of the institution.

The material being returned is from the following individual or Company:

The Hacker Quarterly
P.O. Box 752
Middle Island, NY 11953-0752

You have the right to file an appeal under the Administrative Remedy procedure, but you must make known to me your intention to file within fifteen working days from the date of this memorandum.

Frank Darden (one of the Atlanta hackers) writes: "Well, here I sit. A prisoner of my own hobby. I'm currently being held in a Federal Prison Camp in Talladega, Alabama. I wish I could tell you that Prison Camp is not that bad. Sure, it's not like the prison you see on TV, but it's really sucking. [The above is] what I received instead of *2600*. Apparently your magazine poses a threat to the security of this institution. Let me also say that my hacking days are over. Also, I'd like to add, to any hackers out there, make sure you know what you're getting into. Consider the price you have to pay. Believe me, in my eyes it's not worth it. It was fun while it lasted. Play safe! The Leftist"

We pursued the matter and in July received this response from Warden Roger Scott of the U.S. Department of Justice: "After careful review of your magazine and conferring with the institution's electronic technician, I feel the below listed articles to be improper as they contain information which promotes the illegal use or disruption of coin operated type telephones (COCOT). Since the telephones used by the inmate population are of the coin operated type, I do not feel these articles are appropriate for reading by the inmates: 'COCOT Troubles' on Page 24 describes how to make unauthorized calls from COCOT type telephones. 'Another Method' on Page 26 describes how to make unauthorized calls from COCOT type phones without charges and how to disrupt the operation of the phone. 'Suggestions' on Page 27 describes how to make illegal telephone calls with the help of recorded tones and by use of two telephones. Based on these three articles, I feel I have no alternative but to stand by my previous decision to reject this issue of your *2600* magazine."

The "articles" he refers to are, of course, actually letters. We think it's very unlikely that a prison would have COCOTs. It's very likely, though, that he doesn't even know what a COCOT is and is just assuming that all payphones are the same. In the end, technical ignorance by the authorities prevents Darden from reading the only magazine that talks about the technical ignorance that put him in prison. Sometimes it seems like an endless loop.